Hybrid Decision Vulnerability:
Rethinking Hybrid Threats in Maritime Security

Sabrina Medeiros[*]

The contemporary maritime domain concentrates many of the characteristics that make hybrid threats difficult to identify, attribute and manage. Ports, submarine cables, offshore energy infrastructure, shipping routes, satellite services, navigation systems and maritime surveillance platforms form an increasingly interconnected environment in which physical assets depend on digital systems and institutional responses depend on the quality and circulation of information. Maritime security has long resisted a single definition precisely because it encompasses military power, law enforcement, economic circulation, marine safety, environmental protection and governance practices that overlap without becoming institutionally identical.

Bueger's proposal to understand maritime security through its relations with seapower, marine safety, the blue economy and resilience remains useful because it directs attention to the practices and institutional arrangements through which threats are defined and responses are organized (Bueger, 2015). Germond (2011) likewise emphasizes the coexistence of military, civilian, geopolitical and institutional dimensions in maritime security, while Klein (2011) demonstrates how the law of the sea structures the rights, constraints and jurisdictional choices available to states when they respond to security problems at sea. Hybrid threats enter this already complex environment through the exploitation of dependencies among infrastructures, technologies, legal regimes and organizational responsibilities. Recent work on critical maritime infrastructure reinforces this systemic reading. Neal (2026), examining the post-Nord Stream environment, identifies visibility, surveillance, riskification and securitization dilemmas in which measures intended to improve protection may generate new vulnerabilities. Hofmann, Stockbrügger, and Sill Torres (2026) similarly argue that the strategic relevance of hybrid activities may lie less in direct physical damage than in ambiguity, political effects and cumulative escalation. These contributions shift attention from the isolated incident toward the consequences produced by uncertainty within a connected security environment.

[*] PhD in Political Science from IUPERJ (IESP). Professor of International Relations at Lusófona University in Lisbon. Research Coordinator at the *InterAgency Institute* and Associate Researcher at Portugal's National Defence Institute.

This relational character is especially visible in the contemporary Atlantic. Maritime infrastructures that were once treated primarily as technical or commercial assets have become increasingly central to strategic debates (Bueger and Liebetrau, 2023; Ducruet *et al*., 2010). Submarine communication cables are a clear example. Their physical location on the seabed makes them part of the material geography of the ocean, while their function connects financial transactions, government communications, military systems, digital services and transnational economic activity. Earlier work on submarine cables and cybersecurity in the Atlantic has already shown that their significance arises from this intersection between physical infrastructure, cyber vulnerability and international security, as well as from the legal and political difficulties involved in framing interference with them (Lehto *et al.,* 2026). The same logic extends to ports, offshore energy facilities, navigation services and maritime data systems. Their strategic relevance lies in the network of dependencies that links them to other infrastructures and to the institutions responsible for interpreting disruption and organizing a response.

The literature on hybrid threats offers an increasingly detailed catalogue of the ways in which such dependencies may be exploited (Bjørge; Høiby, 2024; Filipec, 2021; Tagarev, 2018). *The Hybrid CoE Handbook on maritime hybrid threats* develops scenarios ranging from undersea cable cuts and interference with navigation to distant-water fishing, attacks by small craft and contested resource exploitation, explicitly linking these scenarios to legal ambiguity, operational planning and exercises (Giannoulis, 2023). The earlier edition of the handbook had already emphasized the difficulty of producing accurate situational awareness and timely decisions when international law, attribution and malicious behaviour intersect in the maritime domain (Lohela; Schatz, 2019). This is important because hybrid effects are generated through the strategic use of uncertainty as much as through the material effects of an incident. A limited disruption can acquire disproportionate significance when authorities cannot rapidly determine what occurred, who is responsible, which legal framework applies or which organization has the mandate to act (Giannoulis, 2023).

Such dynamics are better understood when maritime security is treated as a complex security system. Complexity in this context refers to the interaction of technological, physical, human, organizational, regulatory and geopolitical components whose effects are not necessarily linear or confined to the point at which an incident originates. A disruption affecting a cable landing station, a port management system or a navigation service can alter the

availability and reliability of information, reshape situational awareness, complicate attribution and change the conditions under which civilian authorities, armed forces, law-enforcement agencies, regulators and private operators coordinate their response (Giannoulis, 2023). These effects can move across institutional and technological boundaries, creating feedback loops and delays that were not evident in the initial event. This perspective is consistent with broader approaches to ocean governance that emphasize multilevel cooperation and the coexistence of security, regulation, development and institutional coordination in maritime spaces (Carvalho *et al*., 2024; Germond; Germond-Duret, 2016).

The Brazilian and South Atlantic experience reinforces the value of this approach. Research on ocean governance involving the Brazilian Navy has shown how the expansion of illicit maritime activities and the growing awareness of crimes at sea have stimulated interagency operations and multinational cooperation, producing governance arrangements in which defence institutions interact with civilian agencies and other actors across several levels (Carvalho *et al.,* 2024). The evolution of the Coordination of the South Atlantic Maritime Area, CAMAS, offers another example. Its contemporary role depends less on a single command structure than on the capacity to sustain information sharing, situational awareness, technical cooperation and regular interaction among South American maritime actors. As an example, CAMAS is representing a community of security practice and a technical sub-regime whose resilience derives from institutional adaptation and from its capacity to maintain cooperation across political changes (Medeiros; Moreira, 2025). The case matters for the discussion of hybrid threats because it shows that maritime security responses are produced through networks of institutions and practices whose effectiveness depends on the circulation, interpretation and validation of information.

Besides the natural adaptative conditioners, maritime authorities may initially have limited means of determining whether an anomalous event results from technical failure, accident, criminal activity, deliberate sabotage or an operation associated with a state actor. Several explanations may remain plausible during the early stages of a crisis, while evidence is incomplete and organizations interpret the available information according to distinct mandates, operational cultures and legal responsibilities. Hybrid action can exploit the interval between detection, interpretation, attribution and response, prolonging uncertainty or introducing contradictory signals into the decision environment. The legal dimension is particularly significant at sea because jurisdiction depends on location, flag, coastal-state rights, vessel status and the character of the conduct involved. Klein's work (2011) on maritime

security and the law of the sea demonstrates how questions of jurisdiction and enforcement shape state responses across a wide range of maritime threats, while recent work on MDA similarly stresses that information only becomes operationally useful when competent actors possess both the willingness and the legal authority to act (Schultheiss, 2026).

Hybrid Decision Vulnerability

This intersection between systemic disruption and decision-making provides the basis for the concept of hybrid decision vulnerability. The term refers to the susceptibility of a decision-making ecosystem to compounded interference across physical infrastructure, digital and data systems, cognitive processes and institutional arrangements, resulting in degraded situational awareness, attribution, coordination or timely response. The concept is intended to capture the interaction among these elements rather than to establish another taxonomy of hybrid instruments. Its analytical object is therefore the chain through which an event becomes actionable knowledge: detection, data transmission, interpretation, attribution, institutional coordination and decision.

Maritime infrastructures are connected to digital environments exposed to cyber intrusion, data poisoning, spoofing and manipulation of AIS or GNSS information; these disturbances affect the informational environment in which decision-makers confront contradictory signals, uncertainty and attribution problems; interpretation then takes place within institutional architectures characterized by distributed responsibilities and uneven capacities for information sharing, civil-military coordination and public-private cooperation (Androjna; Perkovič, 2021). Hybrid decision vulnerability emerges when interference in one or several of these layers propagates through the decision ecosystem and reduces its capacity to transform information into sufficiently reliable and timely action. The analytical distinction is important because physical damage and decision degradation need not be proportional. A relatively limited incident can have significant strategic effects when it produces prolonged uncertainty, competing interpretations or institutional paralysis.

Maritime Domain Awareness provides an especially important empirical setting for observing this process. MDA has evolved from vessel tracking toward a broader effort to understand activities, infrastructures and conditions that may affect security, safety, the economy or the marine environment. Schultheiss shows that contemporary platforms such as SeaVision, IORIS, Skylight and Global Fishing Watch combine satellite imagery, AIS, synthetic aperture radar, vessel registries and other sources, often using artificial intelligence

to detect anomalous behaviour and support maritime agencies (Schultheiss, 2026). His analysis is particularly relevant because it places institutional integration at the centre of technological effectiveness. The usefulness of these platforms depends on the networks of agencies, regional organizations and legal instruments through which information is shared and converted into action. Lack of interoperability, restrictions on information sharing, jurisdictional uncertainty and unequal access to technological capabilities can therefore limit the operational value of highly sophisticated systems.

This point connects directly with the increasing use of artificial intelligence in maritime security. Recent research on AIS-based anomaly detection demonstrates the growing capacity of machine-learning systems to identify unusual vessel trajectories and patterns within very large datasets (Liang *et al*., 2024; Ribeiro *et al*., 2023). Similar work in multimodal maritime surveillance combines AIS with radar, satellite imagery, acoustic signatures and other sensor inputs to improve anomaly detection and address practices such as spoofing and dark-vessel activity. Current European initiatives illustrate how quickly this integration is becoming operational. VIGIMARE, a Horizon Europe project involving infrastructure operators, research institutes and technology providers, combines satellite imagery, fibre-optic sensing, AIS tracking and AI-based anomaly detection in a shared operational picture for operators and authorities (European Commission, 2026; Hartikainen, 2025).

Such developments expand the ability to identify anomalies, but they also deepen dependence on data integrity, sensor reliability, information-sharing arrangements and the assumptions embedded in automated analytical systems. In cyber-physical maritime environments, interference with one data stream can alter the representation of an event even when the wider surveillance system continues to function. AI is therefore best understood here neither as an autonomous category of hybrid threat nor as an inherently resilient solution. It is a capability embedded within the decision ecosystem whose security value depends on the integrity of the data, institutions and human judgments surrounding it. The question of resilience consequently extends from the protection of infrastructure toward the reliability of the informational chain through which institutions construct situational awareness.

This is also where the discussion of AI needs to remain connected to decision-making rather than to technological performance alone. An algorithm may correctly detect an anomaly without producing an effective security response if the information cannot be shared, if agencies disagree over attribution, if the responsible authority lacks jurisdiction or if the event falls between established institutional mandates. This vulnerability is particularly evident when

digital navigation systems are manipulated, as the spoofing of Automatic Identification System (AIS) or Global Navigation Satellite System (GNSS) signals directly degrades maritime situational awareness and misleads automated detection tools (Androjna; Perkovič, 2021). Conversely, a technically imperfect system may still contribute to resilience when organizations possess redundant sources of information, established procedures for verification and channels for rapid coordination. Schultheiss's recent analysis of MDA platforms is especially useful on this point because it identifies the confluence of information, capable actors and jurisdiction as a condition for effective maritime action (Schultheiss, 2026). Hybrid decision vulnerability can therefore be understood as a problem located in the relations connecting technological observation, institutional interpretation and authority to respond.

From Vulnerability to Decision Resilience

The complexity of these relations creates a methodological challenge. Conventional risk assessments can identify exposed assets, likely hazards and organizational responsibilities, yet many vulnerabilities become visible only when institutions are required to act under changing conditions. Simulation and wargaming provide a particularly useful environment for examining this dynamic because they make it possible to manipulate the informational and institutional conditions under which decisions are produced. Scenarios can introduce incomplete intelligence, contradictory sensor data, infrastructure failures, cyber incidents, changes in legal status, time pressure and adversarial adaptation while observing how participants interpret the situation and negotiate a response. In this sense, simulation creates an analytical bridge between complex-systems approaches and the empirical study of decision behaviour. This use of simulation is consistent with a broader research agenda in which simulations are treated as structured methods for observing decision-making, negotiation and institutional interaction.

This orientation is especially suited to hybrid-threat analysis because ambiguity, incomplete information and changing actor incentives are difficult to reproduce through static analytical models. Applied to maritime security, simulated decision-making can expose how vulnerabilities propagate across the decision ecosystem. A scenario involving a suspected cable disruption, for instance, can vary the quality of technical evidence, the presence of suspicious vessel activity, the reliability of AIS data, the availability of satellite imagery, the legal status of the vessel involved and the degree of agreement among civilian and military authorities. This specific variable design aligns with contemporary technical assessments showing that subsea

telecommunication networks are increasingly vulnerable to sophisticated cyber threats and targeted physical-digital interference (Hartikainen, 2025; Lehto, Julkunen; Hartikainen (2026). The resulting exercise allows analysts to observe how participants construct situational awareness, when they begin to attribute responsibility, which information they consider authoritative, how competing institutional mandates are reconciled and how uncertainty affects the willingness or capacity to act. The analytical value lies in the sequence of decisions and interactions through which the crisis is understood. Such an approach can reveal thresholds, bottlenecks, coordination gaps and feedback effects that are difficult to identify when infrastructures, agencies or technologies are assessed separately.

The Hybrid CoE's own work points in a similar direction by designing maritime hybrid-threat scenarios explicitly for policy development, operational planning and exercises (Giannoulis, 2023). This convergence between conceptual analysis and exercise design suggests that simulation can become an important instrument for evaluating decision resilience. Decision resilience concerns the capacity of a complex security system to preserve sufficiently reliable processes of detection, interpretation, coordination and action during disruption and deliberate uncertainty. It depends on technological redundancy and infrastructure protection, but also on information-sharing arrangements, independent means of verification, institutional interoperability, legal preparedness, human oversight of AI-supported systems and established channels of cooperation among military, civilian, law-enforcement, regulatory and private actors. Exercises can examine how these capacities function together and whether formal coordination arrangements remain effective when evidence is incomplete and an adversary adapts its behaviour.

The South Atlantic provides a particularly relevant environment in which to apply this framework because its maritime security architecture combines extensive sea spaces, offshore resources, major ports, submarine cable networks, transnational maritime crime and considerable variation in technological and institutional capacity. The region already contains cooperative arrangements that can support situational awareness and coordination, including CAMAS, as well as bilateral and multilateral initiatives connecting South American and West African actors. This architecture reflects a complex multi-level governance structure where major ports and shipping networks operate under uneven national and regional regulatory frameworks (Carvalho et al., 2024; Ducruet *et al.,* 2010). These institutional differences affect the ability to identify and respond to hybrid interference because resilience depends on the weakest as well as the strongest links in regional information and coordination networks.

This regional perspective also helps avoid the assumption that concepts and frameworks developed in the Baltic, Arctic or wider Euro-Atlantic area can simply be transferred to the South Atlantic. The Hybrid CoE scenarios provide valuable analytical and legal instruments, yet their operational implications are shaped by institutional density, alliance structures, surveillance capabilities, legal coordination and access to technology. The South Atlantic contains a different pattern of political relations and security practices, and its maritime governance has developed through a combination of national initiatives, technical sub-regimes, interagency cooperation and selective regional coordination. This variance underscores that maritime security and ocean governance are fundamentally contextual, shaped by regional political spaces rather than universal security doctrines (Bueger, 2015; Germond; Germond-Duret, 2016). Simulation offers a way to examine the portability of hybrid-threat frameworks under these different conditions because scenarios can preserve a common analytical problem while varying actors, resources, legal arrangements, information systems and coordination mechanisms.

Hybrid decision vulnerability is therefore useful as a concept linking three strands of analysis that have often developed separately: maritime security as a field of interconnected practices and jurisdictions, technological systems for maritime awareness, and simulated decision-making under conditions of uncertainty. The first establishes the institutional and geopolitical complexity of the maritime domain; the second demonstrates the growing dependence of security actors on interconnected data and surveillance systems; the third provides a method for observing how institutions behave when those systems are degraded, manipulated or contested. This connection is particularly important for contemporary maritime security because a technically successful attack is only one possible route through which strategic effects can be produced. Delays in attribution, conflicting institutional interpretations, uncertainty about jurisdiction and failures of coordination may also shape the consequences of an incident.

The integrity of maritime decision-making should therefore be treated as part of critical infrastructure resilience. Physical infrastructure, digital systems, data, human interpretation and institutional coordination participate in the production of situational awareness and response, and disturbances can propagate through these relationships in ways that amplify limited incidents or prolong uncertainty. A complex-systems perspective makes these interactions analytically visible, while simulation provides a means of observing how they

unfold dynamically. For the South Atlantic, this approach is particularly useful because it allows existing cooperative arrangements, technological asymmetries and interagency practices to be incorporated into the analysis of hybrid threats without assuming a single regional model. It also suggests a practical agenda for defence institutions. Assessments of resilience should examine whether actors can preserve four connected functions under deliberate uncertainty: sensing changes in the environment, interpreting information with sufficient reliability, coordinating across institutional boundaries, and deciding and acting within a strategically relevant timeframe. This systemic approach shifts the focus from physical protection alone to the broader resilience of the operational and legal frameworks that govern subsea and offshore spaces (Bueger; Liebetrau, 2023; Neal, 2026).

Simulation-based exercises can test these functions by varying data reliability, attribution, jurisdiction, time pressure and institutional access to information. The resulting research agenda places decision resilience at the intersection of maritime security, critical infrastructure protection, artificial intelligence and institutional cooperation. Hybrid decision vulnerability provides the conceptual link among these domains by directing attention to the points at which interference becomes decision degradation. Ultimately, building this capacity requires moving beyond static organizational mandates toward collaborative preparedness models that integrate civilian, military, and private capabilities (Borch; Heier, 2024). Protecting maritime security in an increasingly connected environment consequently requires preserving not only the operation of critical assets, but also the institutional and informational capacity to understand disruption and respond before uncertainty itself produces strategic advantage.

REFERENCES

ANDROJNA, A.; PERKOVIČ, M. Impact of spoofing of navigation systems on maritime situational awareness. **Transactions on Maritime Science**, v. 10, n. 2, p. 361–373, 2021. DOI: 10.7225/toms.v10.n02.w08.

BJØRGE, N. M.; HØIBY, M. Contemporary research on hybrid threats: status and future avenues. *In:* BORCH, O. J.; HEIER, T. (ed.). **Preparing for Hybrid Threats to Security**: Collaborative Preparedness and Response. [S. l.]: Routledge, 2024. p. 13–35. DOI: 10.4324/9781032617916-3.

BORCH, O. J.; HEIER, T. (ed.). **Preparing for Hybrid Threats to Security**: Collaborative Preparedness and Response. 1st ed. [S. l.]: Routledge, 2024. DOI: 10.4324/9781032617916.

BUEGER, C. What is maritime security? **Marine Policy**, v. 53, p. 159–164, 2015. DOI: 10.1016/j.marpol.2014.12.005.

BUEGER, C.; LIEBETRAU, T. Critical maritime infrastructure protection: what's the trouble? **Marine Policy**, v. 155, art. 105772, 2023.

CARVALHO, C. A. de; SILVA, D. D. da; MEDEIROS, S. E. Multilevel cooperation on behalf of the ocean governance: the Brazilian Navy case study. *In:* JONES, C. (ed.). **Governing Oceans**: Policy Development, Implementation and Evaluation. [S. l.]: Edward Elgar, 2024. p. 100–119. DOI: 10.4337/9781035315598.00013.

DUCRUET, C.; ROZENBLAT, C.; ZAIDI, F. Ports in multi-level maritime networks: evidence from the Atlantic (1996–2006). **Journal of Transport Geography**, v. 18, n. 4, p. 508–518, 2010. DOI: 10.1016/j.jtrangeo.2010.03.005.

EUROPEAN COMMISSION. **Vigilant Maritime Surveillance of Critical Submarine Infrastructure (VIGIMARE)**: periodic reporting for period 1. CORDIS, Horizon Europe, Project 101168016, 2026. Available at: https://cordis.europa.eu/project/id/101168016/reporting.

FILIPEC, O. Preventing hybrid threats: from identification to an effective response. **European Studies**, v. 8, n. 1, p. 17–38, 2021. DOI: 10.2478/eustu-2022-0063.

GERMOND, B. The EU's security and the sea: defining a maritime security strategy. **European Security**, v. 20, n. 4, p. 563–584, 2011. DOI: 10.1080/09662839.2011.635648.

GERMOND, B.; GERMOND-DURET, C. Ocean governance and maritime security in a placeful environment: the case of the European Union. **Marine Policy**, v. 66, p. 124–131, 2016. DOI: 10.1016/j.marpol.2016.01.010.

GIANNOULIS, G. (ed.). **Handbook on Maritime Hybrid Threats**: 15 Scenarios and Legal Scans. Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2023. (Hybrid CoE Paper, 16). Available at: https://www.hybridcoe.fi/publications/hybrid-coe-paper-16-handbook-on-maritime-hybrid-threats-15-scenarios-and-legal-scans/. Accessed on: 25 Aug. 2026.

HARTIKAINEN, H. **Technical Cyber Threats in Undersea Infrastructure**. 2025. Master's thesis – University of Jyväskylä, Jyväskylä, 2025.

HOFMANN, D.; STOCKBRÜGGER, J.; SILL TORRES, F. Assessing hybrid threats to critical infrastructure through morphological analysis and escalation phases. **Proceedings of the International ISCRAM Conference**, v. 23, 2026. DOI: 10.59297/wg9ee247.

KLEIN, N. **Maritime Security and the Law of the Sea**. Oxford: Oxford University Press, 2011. DOI: 10.1093/acprof:oso/9780199566532.001.0001.

LEHTO, M.; JULKUNEN, P.; HARTIKAINEN, H. Cyber security in the subsea telecommunication cable networks. **The Proceedings of the International Conference on**

Cyber Warfare and Security, v. 21, n. 1, p. 212–221, 2026. DOI: 10.34190/iccws.21.1.4505.

LIANG, M.; WENG, L.; GAO, R.; LI, Y.; DU, L. Unsupervised maritime anomaly detection for intelligent situational awareness using AIS data. **Knowledge-Based Systems**, v. 284, art. 111313, 2024. DOI: 10.1016/j.knosys.2023.111313.

LOHELA, T.; SCHATZ, V. (ed.). **Handbook on Maritime Hybrid Threats**: 10 Scenarios and Legal Scans. Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2019. (Hybrid CoE Working Paper, 5).

MEDEIROS, S. E.; MOREIRA, W. de S. Protecting South America's Atlantic waters: a closer look at maritime security and CAMAS. *In:* LEANDRO, F. J. B. S. *et al.* (ed.). **The Palgrave Handbook on Geopolitics of Brazil and the South Atlantic**. Singapore: Palgrave Macmillan, 2025. p. 1021–1035. DOI: 10.1007/978-981-95-1169-3_45.

NEAL, A. W. After Nord Stream: four security dilemmas in critical maritime infrastructure protection. **International Affairs**, v. 102, n. 1, p. 207–225, 2026. DOI: 10.1093/ia/iiaf229.

RIBEIRO, C. V.; PAES, A.; OLIVEIRA, D. de. AIS-based maritime anomaly traffic detection: a review. **Expert Systems with Applications**, v. 231, art. 120561, 2023. DOI: 10.1016/j.eswa.2023.120561.

SCHULTHEISS, C. Satellites, AI and information-sharing platforms for the maritime domain: have new technologies revolutionized maritime security? **International Affairs**, v. 102, n. 3, p. 925–948, 2026. DOI: 10.1093/ia/iiag037.

TAGAREV, T. Hybrid warfare: emerging research topics. **Information & Security**: An International Journal, v. 39, n. 3, p. 289–300, 2018. DOI: 10.11610/isij.3924.