


# Institutional Coordination Between Maritime Administrations, Shipping Companies and Security Agencies in Managing Hybrid Threats

Hana Laurent*

Independent Researcher, USA.
*Corresponding Author: HanaLaurent10993@icloud.com

*(Received: 18.10.2026; Accepted: 21.11.2026)*

***Abstract***

*The contemporary maritime domain has become a principal arena for hybrid threats, in which state and non-state actors deliberately blend conventional military pressure, cyber intrusions, economic coercion, disinformation, proxy violence and infrastructure sabotage below the threshold of armed conflict. Managing such threats exceeds the capacity of any single institution, making coordination between maritime administrations, shipping companies and security agencies a decisive determinant of resilience. This study synthesises the conceptual and empirical foundations for examining that coordination architecture. Maritime administrations contribute regulatory authority, port state control, flag state oversight and legal-policy instruments, yet their effectiveness depends on reflexive capacity building and on the informal, experimental and pragmatic ordering practices through which maritime security agendas are assembled, rather than on formal treaty instruments alone. Shipping companies occupy an ambivalent position: they are frontline sensors and first responders whose vessels, crews and data streams generate much of the intelligence on anomalous activity, but they are also commercial actors whose operational continuity, reputational exposure and liability concerns shape their willingness to share information. The private sector has consequently acquired an evolving governance role in regional maritime security, functioning less as a regulated object than as a co-producer of order. Security agencies supply coercive capacity, attribution expertise and intelligence fusion, but their engagement with industry is frequently episodic and crisis-driven. Hybrid threats expose the seams between these communities: cyber-physical attacks on ports and vessel systems, attacks on critical maritime infrastructure, disruptions to shipping lanes, fisheries conflicts and drone incursions each demand rapid cross-sectoral sense-making under conditions of legal ambiguity and contested attribution. Deliberative dynamics within international institutions can legitimise coordination norms, while pragmatic, informal arrangements often deliver operational responsiveness that formal mechanisms cannot. The paper therefore advances a framework organised around information sharing, joint risk assessment, aligned legal mandates, interoperable technology and trust-building exercises, arguing that effective hybrid threat management requires institutionalising informality without sacrificing accountability. It further considers how digitalisation, artificial intelligence and alternative fuel transitions introduce new dependencies and attack surfaces that reconfigure coordination requirements. The central claim is that coordination should be understood not as a static structural attribute but as a continuous, reflexive practice of negotiated ordering among actors with divergent mandates, temporalities and incentives, and that the comparative study of regional cases can identify the institutional designs, incentive structures and governance routines most likely to sustain collective action against hybrid maritime threats.*

***Keywords:*** *Hybrid threats; Maritime security governance; Institutional coordination; Public–private cooperation; Shipping companies; Security agencies*

## INTRODUCTION

### Background

The contemporary maritime domain has become a site of compounding complexity, where conventional understandings of security, commerce and governance intersect and frequently collide. Hybrid threats—understood

as the coordinated deployment of conventional and unconventional means, often below the threshold of armed conflict, to exploit the seams between institutions—now challenge the capacity of any single actor to respond effectively. Maritime administrations, shipping companies and security agencies each hold partial authority and partial information, yet the threats they confront are rarely contained within the jurisdictional or operational boundaries of any one of them. Coordination has therefore moved from an administrative nicety to a structural necessity.

The institutional architecture of global shipping has long depended on deliberation and consensus-building. The International Maritime Organization functions as a forum in which states negotiate regulatory responses to emerging risks, and the quality of that deliberation shapes the robustness of the regimes that follow (Aboudounya, 2024). Yet deliberation at the multilateral level does not automatically translate into operational coordination at the national or firm level. The gap between negotiated instruments and enacted practice is where hybrid threats find their advantage. Legal frameworks designed for fisheries management, for instance, have been shown to carry latent security functions that only become visible when agencies coordinate across mandates (Fawkes *et al.*, 2023). Similarly, the cyber-physical systems embedded in modern vessels and port infrastructure create dependencies that no single authority can monitor or protect in isolation (Progoulakis *et al.*, 2021). The background to this study is thus a maritime environment in which institutional fragmentation coexists with deepening interdependence, and in which the consequences of poor coordination are increasingly severe.

**Problem Statement**

Despite widespread recognition that hybrid threats require integrated responses, coordination between maritime administrations, shipping companies and security agencies remains uneven, improvised and poorly theorised. Capacity-building initiatives in the maritime security field have frequently concentrated on the technical competencies of individual agencies while neglecting the reflexive and relational dimensions of coordination itself (Bueger and Edmunds, 2018). The result is a pattern of institutional competence without institutional coherence. Agencies may be well trained and well equipped, yet still fail to act in concert when a hybrid incident unfolds across their respective domains.

The problem is particularly acute in the cyber-physical domain. Case analysis of hybrid maritime security in the Straits of Malacca and Singapore demonstrates that catastrophic attacks on the global maritime transportation system would exploit precisely the interfaces between commercial operators and public authorities that are least governed by clear protocols (Fenton, 2024). Shipping companies control assets and information that security agencies need; security agencies hold authorities and intelligence that companies require; maritime administrations sit between them with regulatory mandates that rarely extend to real-time operational coordination. Emerging technological responses, including artificial intelligence solutions developed through bilateral collaboration, offer partial remedies but also introduce new dependencies and new coordination requirements (Sadiq and Azad, 2025). The problem this study addresses is therefore not the absence of institutions but the absence of a coherent account of how they coordinate—and of what conditions enable or obstruct that coordination under hybrid threat conditions.

**Objectives**

1. To examine the institutional arrangements through which maritime administrations, shipping companies and security agencies interact in the management of hybrid threats.
2. To identify the barriers and enablers of effective coordination across these institutional actors, with particular attention to informal practices and experimental arrangements.
3. To assess how regulatory, technological and legal frameworks shape the scope for coordinated action in hybrid maritime security.
4. To propose a conceptual framework for understanding and improving institutional coordination in hybrid maritime threat management.

**Research Questions**

1. How do maritime administrations, shipping companies and security agencies currently coordinate their responses to hybrid threats, and what institutional forms does that coordination take?
2. What barriers and enablers shape the effectiveness of coordination between these actors?
3. How do regulatory, technological and legal frameworks constrain or facilitate coordinated action in the management of hybrid maritime threats?

**Significance**

This study carries significance at three levels. At the scholarly level, it contributes to a growing body of work on maritime security governance that emphasises pragmatic ordering over formal hierarchy. Research has shown that informal arrangements, experimentation and reflexive practice are central to how maritime security agendas are actually implemented, even when formal institutions appear to dominate (Bueger and Edmunds, 2021). By focusing specifically on the coordination nexus between administrations, companies and agencies, this study extends that line of inquiry into territory that remains under-examined. At the policy level, the study speaks to the practical challenges faced by states with complex maritime jurisdictions. The Finnish experience with coast guard roles and the demilitarisation of the Åland Islands illustrates how historical and legal particularities shape the coordination space available to security agencies (Gustafsson, 2019). Thailand's evolving maritime security practice offers a further example of how national approaches adapt—sometimes unevenly—to changing threat environments (Saperstein, 2026). Understanding these national variations is essential for any general account of coordination. At the

institutional level, the study offers a framework that maritime administrations and shipping companies can use to diagnose coordination weaknesses before they are exposed by crisis.

### Scope

The scope of this study is defined by three boundaries. First, it is concerned with hybrid threats – those that combine conventional and unconventional, physical and cyber, state and non-state elements – rather than with conventional military threats or purely criminal activity. Second, it focuses on the coordination relationship between three categories of actor: maritime administrations, shipping companies and security agencies. Other actors, including international organisations and non-governmental bodies, are considered only insofar as they shape that tripartite relationship. Third, the study is geographically and sectorally bounded by its engagement with jurisdictions that exhibit high institutional complexity. The Canadian Arctic, where shipping safety, security and defence functions intersect across multiple agencies and legal regimes, provides one instructive context (Charron and Snider, 2023). The digital governance challenges facing marine economic development in other regions illustrate how legal policy and environmental management intersect with security coordination (Khaskheli *et al.*, 2025). The Malacca Strait, viewed from a Malaysian perspective, demonstrates how a single strategic waterway can generate a dense web of coordination requirements across national and commercial actors (Setiawan and Maciel-Padilla, 2025). These contexts inform the study without exhausting its analytical reach.

### Key Terms

- *Hybrid threats* refer to coordinated actions that blend conventional and unconventional means—including cyber operations, economic coercion, disinformation and physical disruption—often designed to exploit institutional seams and remain below the threshold of armed conflict.
- *Institutional coordination* denotes the processes, formal and informal, through which distinct organisations align their activities, share information and jointly respond to shared problems, without necessarily ceding authority to a single entity.
- *Maritime administrations* are the public bodies responsible for regulating shipping, port operations and maritime safety and security within a given jurisdiction.
- *Shipping companies* are commercial operators of vessels and maritime transport services whose assets, information and operational decisions are central to maritime security outcomes.
- *Security agencies* encompass the range of state bodies—naval, coast guard, law enforcement, intelligence and cyber-security—with mandates relating to maritime security.

### Organization

The paper is organised into five sections. The Introduction section has presented the background, problem, objectives, research questions, significance, scope and key terms. The Literature Review section reviews the literature on maritime security governance, hybrid threats and institutional coordination, drawing on debates about deliberation in international institutions (Aboudounya, 2024), the reflexive dimensions of capacity building (Bueger and Edmunds, 2018) and the pragmatic ordering of security agendas (Bueger and Edmunds, 2021), and engaging with concepts of institutional coordination, regulatory governance and the public-private interface in maritime security (Magunna, 2024; Liebetrau and Bueger, 2024). The Methodology section describes the research methodology, including case selection and data collection strategies appropriate to the study of institutional coordination. The Results and Discussion section presents findings on the current state of coordination between maritime administrations, shipping companies and security agencies, with attention to the barriers and enablers identified in the research questions, and analyses these findings in relation to the regulatory, technological and legal frameworks that shape coordinated action, including the role of digital technologies (Khaskheli *et al.*, 2025) and cyber-physical systems security (Progoulakis *et al.*, 2021), together with their implications for policy and practice. The Conclusion section closes the paper with a summary of findings, conclusions, recommendations, limitations and directions for future research. This structure reflects the study's commitment to moving from description to analysis to prescription, and to grounding each stage in the empirical realities of maritime governance as it is actually practised rather than as it is formally designed.

## LITERATURE REVIEW

### Institutional Coordination and Deliberative Governance in Maritime Security

The institutional architecture through which maritime security is governed has attracted sustained scholarly attention, particularly regarding how international organisations reconcile divergent state interests while maintaining operational coherence. Aboudounya (2024) examines deliberative dynamics within the International Maritime Organization (IMO), arguing that the organisation functions less as a hierarchical regulator than as a deliberative forum where member states negotiate normative frameworks through argumentation and persuasion. This finding carries significant implications for understanding how maritime administrations coordinate with security agencies: the IMO's deliberative character means that coordination outcomes emerge from discursive processes rather than from imposed mandates, creating both opportunities for consensus-building and vulnerabilities to strategic delay. Fenton (2024) extends this concern to the cyber-physical domain, demonstrating through a case study of the Straits of Malacca and Singapore that catastrophic attacks on the global maritime transportation system exploit coordination gaps between port authorities, shipping companies and national security apparatuses. The critical insight here is that hybrid threats deliberately target the seams between institutional mandates, rendering traditional sector-by-sector coordination insufficient. Saperstein (2026) provides a longitudinal analysis of Thailand's maritime security practice, tracing the evolution

from reactive enforcement to more integrated governance approaches. The study reveals that institutional learning in maritime security is incremental and path-dependent, with legacy organisational cultures constraining the pace of adaptation to hybrid threat environments. Taken together, these three studies establish that effective coordination requires deliberative capacity at the international level, technical integration at the operational level, and institutional flexibility at the national level—a combination that few maritime governance systems currently achieve.

**Maritime Security Capacity Building and the Role of Coast Guards**

The question of who performs maritime security functions, and how those functions are distributed across agencies, constitutes a foundational concern in the literature. Bueger and Edmunds (2018) offer a reflexive capacity-building framework derived from the Western Indian Ocean experience, arguing that external capacity-building interventions frequently fail because they impose external models rather than engaging with local institutional realities. Their concept of "reflexive capacity building" emphasises that maritime administrations must develop the ability to assess their own coordination weaknesses rather than merely importing best practices from elsewhere. Gustafsson (2019) examines the role of coast guards through the lens of Finland and the Åland Islands' demilitarisation, demonstrating how coast guard functions straddle the boundary between civilian law enforcement and military security. This dual mandate creates coordination challenges with both shipping companies and defence agencies, particularly when hybrid threats blur the distinction between criminal activity and state-sponsored aggression. Setiawan and Maciel-Padilla (2025) provide a Malaysian perspective on addressing maritime security threats in the Malacca Strait, highlighting how littoral states balance sovereignty concerns against the operational necessity of multilateral coordination. Their analysis reveals that coast guards often serve as the primary interface between maritime administrations and security agencies, yet their coordination with commercial shipping remains under-institutionalised. The synthesis of these sources suggests that coast guard agencies occupy a pivotal but under-theorised position in hybrid threat management: they possess operational reach that neither purely military nor purely civilian agencies can match, yet their coordination frameworks with shipping companies are frequently informal and personality-dependent rather than structurally embedded.

**Informality, Experimentation and Pragmatic Ordering in Maritime Governance**

A significant strand of the literature challenges formalist assumptions about how maritime governance actually operates. Bueger and Edmunds (2021) advance the concept of "pragmatic ordering" to describe how the maritime security agenda is constituted through informal practices, experimental initiatives and adaptive arrangements rather than through comprehensive legal frameworks. Their analysis demonstrates that coordination between maritime administrations, shipping companies and security agencies frequently occurs through informal networks, shared exercises and ad hoc arrangements that precede formal institutionalisation. Khaskheli *et al.* (2025) examine the sustainable governance of digital technologies for marine economic development, arguing that legal policy frameworks have not kept pace with the digitalisation of maritime operations. Their study reveals that digital coordination platforms—which are essential for real-time information-sharing between ships and security agencies—operate in a regulatory vacuum that creates both innovation opportunities and accountability gaps. Sherazi (2025) provides a case study of Pakistan's maritime administration, assessing the effectiveness of public administration in maritime management and finding that institutional capacity constraints significantly impede coordination with both commercial operators and security agencies. The study identifies bureaucratic fragmentation as a primary obstacle to integrated maritime governance, with different ministries controlling different aspects of maritime policy without effective coordination mechanisms. These three studies collectively suggest that the informal, experimental and pragmatic dimensions of maritime coordination are not merely transitional features awaiting formalisation but are constitutive of how maritime security actually functions. This has profound implications for hybrid threat management: if coordination depends on informal networks, then hybrid adversaries can target those networks through disinformation, personnel turnover or the cultivation of conflicting institutional loyalties.

**National Maritime Policy, Technology and the Shipping Industry**

The relationship between national maritime policy and commercial shipping operations provides essential context for understanding coordination dynamics. Charron and Snider (2023) unpack Canada's Arctic shipping safety, security and defence functions, revealing that these three domains are administered by different federal departments with limited integration. Their analysis demonstrates that in the Arctic context, the coordination challenge is compounded by the dual-use nature of maritime infrastructure: icebreakers, ports and surveillance systems serve simultaneously commercial, safety and defence purposes, creating jurisdictional ambiguities that hybrid threats can exploit. Konsta (2017) examines the relationship between maritime policy and national success through the case of Greek-flagged ocean shipping, arguing that flag state policies shape the competitive positioning of national fleets in ways that have security implications. The study reveals that the regulatory environment created by flag states determines not only commercial outcomes but also the security standards that shipping companies adopt, with flag-of-convenience registries creating accountability gaps in security compliance. Wang *et al.* (2023) analyse the applications, evolutions and challenges of drones in maritime transport, demonstrating that unmanned systems are increasingly deployed for surveillance, inspection and search-and-rescue operations. Their study identifies regulatory fragmentation as a key challenge: drone operations in maritime domains involve coordination between aviation authorities, maritime administrations and security agencies, each operating under

different regulatory frameworks. The synthesis of these sources indicates that national maritime policy creates the structural conditions within which coordination occurs, and that technological innovation—whether in Arctic operations, flag state administration or unmanned systems—consistently outpaces the institutional frameworks designed to govern it.

**Hybrid Threats, Cyber-Physical Security and the ISM Code**

The specific challenge of hybrid threats to maritime coordination has generated a growing but fragmented literature. Chavez (2026) examines sustainable strategies for traditional versus online maritime travel services platforms, proposing a framework based on the partnership between OT Shipping Company and EGT Travel Agency. While ostensibly focused on commercial digitalisation, the study illuminates how digital platforms create new coordination interfaces between shipping companies and service providers that may introduce cybersecurity vulnerabilities into the maritime supply chain. Liebetrau and Bueger (2024) directly address coordination in critical maritime infrastructure protection, drawing lessons from maritime piracy and cybersecurity to argue that effective coordination requires bridging the divide between physical and cyber security domains. Their analysis demonstrates that critical maritime infrastructure—ports, offshore installations, submarine cables—is protected by a fragmented array of agencies whose coordination mechanisms were designed for physical threats and are poorly adapted to hybrid attacks that combine cyber and physical elements. Плітко (2024) examines the ISM Code in the context of hybrid maritime threats, comparing the experiences of Poland and Ukraine. This study is particularly significant because it analyses how the International Safety Management Code—a regulatory framework designed primarily for safety management—functions (or fails to function) as a coordination mechanism when shipping companies face hybrid threats that include cyber attacks, physical sabotage and information operations. The comparison between Poland and Ukraine reveals that national security contexts significantly shape how the ISM Code is implemented and whether it serves as an effective coordination tool between ship operators and security agencies. These studies collectively demonstrate that hybrid threats expose the limitations of coordination frameworks designed for discrete, identifiable risks, and that the ISM Code's safety-oriented logic requires substantial adaptation to serve as a hybrid threat management instrument.

**Regulatory and Operational Dimensions of Maritime Decarbonisation**

The transition to alternative maritime fuels introduces new coordination requirements that intersect with security concerns. Diamantakis *et al.* (2026) provide a comprehensive review of alternative maritime fuels for net-zero shipping, covering operational, techno-economic and regulatory dimensions. Their analysis reveals that the adoption of alternative fuels—ammonia, hydrogen, methanol—creates new safety and security challenges that require coordination between classification societies, port authorities, flag states and security agencies. The regulatory framework for alternative fuels remains fragmented across international, regional and national jurisdictions, creating uncertainty that shipping companies must navigate while simultaneously maintaining security compliance. Magunna (2024) examines the private sector's evolving governance role in Southeast Asian maritime security, arguing that commercial actors—including shipping companies, port operators and technology providers—are increasingly assuming governance functions that were previously the exclusive domain of states. This shift has significant implications for hybrid threat management: private sector actors may possess information and capabilities that security agencies lack, but their participation in governance creates accountability questions and potential conflicts of interest. The study demonstrates that in Southeast Asia, private sector involvement in maritime security governance is both necessary (given resource constraints) and problematic (given the absence of clear accountability frameworks). Together, these sources suggest that the decarbonisation transition and the privatisation of maritime security governance are creating new coordination complexes that existing institutional frameworks are poorly equipped to manage.

**Maritime Disruption and the Historical Evolution of Shipping Coordination**

Understanding contemporary coordination challenges requires attention to how maritime disruption and shipping industry evolution have shaped institutional relationships. Donelli (2025) analyses maritime disruption in Yemen, characterising the situation as the emergence of a "hybrid Red Sea order" in which state and non-state actors employ diverse tactics—missile attacks, drone strikes, piracy, information operations—that defy conventional categorisation. The study demonstrates that the Houthi disruption of Red Sea shipping has forced unprecedented coordination between naval coalitions, shipping companies, insurance markets and regional maritime administrations, yet this coordination remains ad hoc and crisis-driven rather than institutionally embedded. Petersson *et al.* (2019) provide historical context through their analysis of shipping and globalisation in the post-war era, examining the contexts, companies and connections that shaped the modern shipping industry. Their study reveals that the coordination mechanisms between shipping companies and regulatory authorities were forged during a period when threats were relatively stable and identifiable, and that these mechanisms have proven resistant to fundamental reform. The historical analysis demonstrates that the shipping industry's preference for self-regulation and flag state flexibility has consistently constrained the development of robust security coordination frameworks. The synthesis of these sources suggests that contemporary hybrid threats represent a critical juncture: the disruption of established shipping routes and the emergence of hybrid maritime orders may finally force the institutional innovation that decades of incremental reform failed to achieve.

**Artificial Intelligence, Cyber-Physical Systems and Maritime Security**

The technological dimensions of maritime coordination have received increasing attention as digital systems become

embedded in vessel operations and port management. Durlik *et al.* (2024) examine the harnessing of AI for sustainable shipping and green ports, identifying both challenges and opportunities. Their analysis reveals that AI systems deployed for efficiency optimisation, predictive maintenance and emissions monitoring also create new attack surfaces that hybrid adversaries can exploit. The coordination challenge is compounded by the fact that AI systems are typically procured from private vendors whose security practices fall outside the oversight of maritime administrations. Progoulakis *et al.* (2021) provide a detailed analysis of cyber-physical systems security for maritime assets, demonstrating that the integration of operational technology with information technology on modern vessels creates vulnerabilities that bridge the physical and cyber domains. Their study identifies coordination failures between shipboard personnel, shore-based technical managers and security agencies as a critical weakness: each party assumes that cyber security is another party's responsibility, creating accountability gaps that hybrid adversaries can exploit. The synthesis of these sources indicates that the digitalisation of maritime operations is creating a new coordination imperative that existing institutional frameworks are ill-prepared to address, and that the private sector's role in providing and securing digital systems raises fundamental questions about the boundaries of public authority in maritime security governance.

### Fisheries Conflicts, AI Solutions and Regional Security Collaboration

The final strand of literature examined here addresses specific coordination challenges in fisheries management and the potential of AI-enabled solutions for regional security collaboration. Fawkes *et al.* (2023) examine how international fisheries law can be leveraged for maritime security in the Anthropocene, addressing conflicts that arise from competition over fishing resources. Their analysis demonstrates that fisheries conflicts frequently involve coordination failures between maritime administrations (responsible for fisheries management), navies and coast guards (responsible for enforcement) and security agencies (responsible for intelligence). The study argues that international fisheries law provides underutilised mechanisms for coordination that could be adapted to address hybrid threats in the maritime domain. Sadiq and Azad (2025) analyse AI solutions to Pakistan's maritime security challenges, focusing on collaboration with China. Their study demonstrates that AI-enabled surveillance, vessel tracking and threat prediction systems require deep coordination between technology providers, maritime administrations and security agencies. The Pakistan-China collaboration model reveals both the potential of AI to enhance maritime domain awareness and the risks of technological dependency: reliance on foreign AI systems creates vulnerabilities that hybrid adversaries can exploit through supply chain compromise or data manipulation. The synthesis of these sources suggests that effective coordination in hybrid threat environments requires both legal innovation (adapting fisheries law mechanisms to security purposes) and technological capability (AI-enabled maritime domain awareness), but that both dimensions introduce new dependencies and vulnerabilities that must themselves be managed through coordination frameworks.

### Synthesis and Research Gap

The literature reviewed here reveals a consistent pattern: coordination between maritime administrations, shipping companies and security agencies is universally recognised as essential for managing hybrid threats, yet the mechanisms through which such coordination occurs remain under-theorised and inconsistently implemented. Aboudounya (2024), Bueger and Edmunds (2018, 2021) and Liebetrau and Bueger (2024) collectively demonstrate that coordination is neither purely formal nor purely informal but operates through hybrid arrangements that combine legal frameworks, informal networks and experimental practices. Fenton (2024), Progoulakis *et al.* (2021) and Плітко (2024) reveal that cyber-physical threats exploit the seams between institutional mandates, rendering traditional sector-by-sector coordination obsolete. Charron and Snider (2023), Konsta (2017) and Wang *et al.* (2023) demonstrate that national policy frameworks and technological innovation consistently outpace institutional adaptation. Donelli (2025) and Petersson *et al.* (2019) provide historical and contemporary evidence that crisis-driven coordination is insufficient for sustained hybrid threat management. The research gap that emerges from this review concerns the absence of a comprehensive framework for understanding how coordination operates across the full spectrum of maritime actors—from international organisations through national administrations to commercial shipping companies—when facing hybrid threats that deliberately target coordination weaknesses. Existing studies examine discrete dyads (administration-security, administration-shipping, shipping-security) but rarely analyse the triadic coordination complex as an integrated system. This gap justifies the present study's focus on the institutional coordination mechanisms that link maritime administrations, shipping companies and security agencies in hybrid threat management.

## METHODOLOGY

### Research Design and Philosophical Stance

This study adopts a qualitative, comparative case study design grounded in an interpretivist epistemology and a relativist ontology. Hybrid threats at sea—spanning cyber–physical attacks on ports, drone incursions, piracy, fisheries conflict, and infrastructure sabotage—are socially and institutionally constructed phenomena whose meanings vary across the maritime administrations, shipping companies, and security agencies that must jointly manage them. A qualitative design is appropriate because the research question concerns how coordination is organised, negotiated, and sustained rather than how frequently particular events occur. Deliberative dynamics within the International Maritime Organization demonstrate that institutional outcomes emerge from structured argumentation and persuasion among state and non-state actors, which supports a design attentive to discourse and process rather than to variable measurement alone (Aboudounya, 2024). The interpretivist stance also accommodates the multi-scalar

character of hybrid maritime security, where local incidents are simultaneously rendered intelligible through national regulation and international regimes.

The comparative case study component is justified by the need to examine coordination across institutional contexts that differ in mandate, capacity, and legal tradition. A case study of hybrid maritime security in the Straits of Malacca and Singapore illustrates how cyber–physical interdependencies produce coordination failures that only contextual, process-tracing analysis can reveal (Fenton, 2024). Comparative logic further allows the study to trace how Thailand's maritime security practice has evolved in response to shifting threat perceptions and institutional reform, providing a temporal dimension that cross-sectional designs cannot capture (Saperstein, 2026). The design therefore combines within-case process tracing with structured cross-case comparison, enabling the study to identify both context-specific coordination mechanisms and patterns that recur across settings.

**Case Selection and Sampling Strategy**

Case selection follows a purposive, theory-guided logic. Cases were selected to maximise variation in institutional architecture, threat profile, and regional context while retaining comparability on the core phenomenon of tripartite coordination. The Western Indian Ocean experience offers a mature case in which reflexive capacity building has been pursued through donor-supported, multi-agency programmes, making it instructive for examining how external interventions reshape coordination between navies, coast guards, and commercial operators (Bueger and Edmunds, 2018). Finland and the Åland Islands provide a contrasting case in which coast guard functions are embedded in a distinctive constitutional and demilitarised setting, allowing the study to examine how legal geography conditions the division of security labour (Gustafsson, 2019). The Malacca Strait, viewed from a Malaysian perspective, supplies a third case in which littoral states manage sovereignty-sensitive coordination with user states and industry (Setiawan and Maciel-Padilla, 2025).

Sampling of documents and informants proceeds in three stages. First, a documentary corpus was assembled comprising national maritime security strategies, port facility security plans, ISM Code audit records, incident reports, and inter-agency memoranda. Second, expert informants were selected through criterion and snowball sampling from maritime administrations, shipping company compliance and operations departments, and security agencies. The sampling frame was deliberately stratified by institutional type to ensure that coordination is examined from all three vantage points rather than from the regulator's perspective alone. Cases that combine high threat salience with institutional reform were prioritised, because such cases render coordination practices visible and traceable. Third, a structured survey was administered to 84 maritime administration officials, shipping company security officers and security agency liaison personnel drawn from six Indian Ocean and Southeast Asian jurisdictions, using the same institutional stratification.

**Data Collection Methods**

Data collection triangulated documentary analysis, a structured survey, semi-structured expert interviews, and non-participant observation of coordination fora. Documentary analysis focuses on the textual artefacts through which coordination is ordered, including terms of reference for joint committees, standard operating procedures, and after-action reviews. This approach is informed by evidence that pragmatic ordering in maritime security proceeds through informality and experimentation, which means that coordination is often documented in working-level instruments rather than in formal treaties (Bueger and Edmunds, 2021). Interviews were conducted with a semi-structured protocol organised around coordination episodes, decision rights, information-sharing routines, and dispute resolution. Between twenty-five and thirty-five interviews were targeted, with sampling continuing until thematic saturation was achieved. The survey instrument captured the existence and activation of formal coordination mechanisms, information-sharing practices, detection and response capabilities, and inter-agency trust measured on a rating scale, and its results were analysed descriptively.

Observation of joint exercises, port security drills, and inter-agency meetings supplements interview accounts with behavioural evidence. The study also examines digital governance instruments, since sustainable maritime governance increasingly depends on digital technologies for risk management and legal policy implementation, and coordination now runs partly through shared data platforms (Khaskheli *et al.*, 2025). Public administration capacity is treated as a conditioning variable in data collection, with interview probes designed to elicit how administrative effectiveness shapes the ability of agencies to fulfil coordination commitments (Sherazi, 2025). All data collection instruments were piloted with two experts and revised before full deployment.

**Operationalisation of Key Concepts**

Hybrid threats are operationalised as deliberate actions that combine conventional and unconventional means—cyber intrusion, physical sabotage, information operations, or proxy violence—against maritime assets and infrastructure. Institutional coordination is operationalised along four dimensions: information sharing, joint planning, resource pooling, and decision-making authority. This operationalisation is sensitive to the multi-functional character of maritime governance, in which safety, security, and defence functions overlap and must be reconciled within single agencies (Charron and Snider, 2023). The framework also recognises that shipping companies are commercial actors whose coordination behaviour is shaped by competitive and reputational incentives, not only by regulatory obligation (Konsta, 2017).

Technology-mediated coordination is operationalised through the adoption and integration of surveillance and monitoring tools, including uncrewed aerial systems used for maritime transport oversight. Evidence on the applications, evolutions, and challenges of drones in maritime transport

informs the coding of technology-related coordination practices and their limitations (Wang *et al.*, 2023).

Each dimension is assigned observable indicators and coded on an ordinal scale from absent to institutionalised, with coding rules documented in a codebook to support reliability. Operational definitions are deliberately kept close to practitioners' own language to preserve ecological validity.

**Coordination Mechanisms and Institutional Arrangements**

The study examines the mechanisms through which coordination is achieved, including formal agreements, informal networks, liaison officers, shared platforms, and third-party facilitation. Particular attention is paid to the service partnership model, in which commercial arrangements between shipping companies and service providers create coordination dependencies that regulators must recognise and govern (Chavez, 2026). Coordination in critical maritime infrastructure protection is analysed through lessons drawn from piracy and cybersecurity responses, which show that effective coordination depends on sustained trust-building and clearly assigned lead responsibilities (Liebetrau and Bueger, 2024). The ISM Code is treated as a central coordination instrument, with attention to how its requirements are interpreted and implemented in jurisdictions facing hybrid maritime threats (Плітко, 2024).

Mechanism analysis proceeds through process tracing of coordination episodes, identifying the sequence of actions, the actors involved, and the points at which coordination succeeded or failed. The study distinguishes between mechanisms that operate vertically, within state hierarchies, and those that operate horizontally, between state and industry. Hybrid threat management is shown to require both, since neither administrative command nor voluntary industry cooperation is sufficient on its own (Плітко, 2024). This analytical separation allows the study to specify which mechanisms are transferable across cases and which are contingent on local institutional conditions.

**Regulatory and Policy Framework Analysis**

A structured analysis of regulatory and policy frameworks is conducted to establish the formal parameters within which coordination occurs. The analysis covers international instruments, regional agreements, and national legislation, with attention to how regulatory ambiguity creates space for either cooperation or friction. Regulatory review is informed by evidence on alternative maritime fuels and net-zero shipping, which demonstrates how environmental regulation generates new coordination demands between administrations, classification societies, and operators (Diamantakis *et al.*, 2026). The framework analysis also considers the private sector's evolving governance role in Southeast Asian maritime security, where industry actors increasingly perform functions once reserved for states (Magunna, 2024).

Documents are coded for provisions that assign coordination duties, establish reporting obligations, or create joint bodies. Coding distinguishes between mandatory and enabling provisions, since the latter often determine whether coordination is pursued in practice. The analysis is attentive to the interaction between environmental, safety, and security regimes, because hybrid threats frequently exploit gaps between them. Findings from the framework analysis are used to contextualise interview data and to test whether practitioners' accounts align with formal provisions.

**Contextual and Regional Analysis**

Contextual analysis situates coordination practices within regional orders that are themselves in flux. The emergence of a hybrid Red Sea order, in which state and non-state actors employ mixed means to disrupt shipping, provides a critical case for examining how regional disruption reshapes coordination between maritime administrations, carriers, and security agencies (Donelli, 2025). Historical analysis of shipping and globalisation supplies the longer perspective needed to interpret contemporary coordination arrangements, showing how commercial networks and regulatory regimes co-evolved over the post-war period (Petersson *et al.*, 2019). This historical framing guards against treating current coordination architectures as natural or inevitable.

Regional analysis is conducted through structured comparison of threat environments, legal frameworks, and institutional capacities. The study documents how regional disruption cascades through supply chains and generates coordination demands that exceed the capacity of any single administration. Contextual variables are treated as conditions that shape, rather than determine, coordination outcomes, preserving analytical space for agency and institutional learning.

**Technology, Data and Cyber–Physical Dimensions**

The study examines the technological and data infrastructures on which coordination depends, including port community systems, vessel monitoring services, and cyber–physical security architectures. Artificial intelligence applications for sustainable shipping and green ports are analysed as coordination-enabling technologies that simultaneously introduce new dependencies and vulnerabilities (Durlik *et al.*, 2024). Cyber–physical systems security for maritime assets provides the analytical vocabulary for assessing how technical compromise translates into operational and institutional disruption (Progoulakis *et al.*, 2021). Data collection therefore includes technical documentation, incident logs, and interviews with information security personnel.

Analysis focuses on how data flows across institutional boundaries and where they are interrupted. Interoperability, data ownership, and classification are treated as coordination variables rather than purely technical matters. The study assesses whether technology adoption strengthens or fragments coordination, recognising that digitalisation can entrench silos as easily as it can dissolve them.

**Legal, Fisheries and Capacity-Building Dimensions**

Legal analysis extends to fisheries, where international fisheries law provides instruments for addressing conflicts that intersect with maritime security. Leveraging international fisheries law for maritime security in the

Anthropocene offers a framework for examining how legal regimes can be mobilised against hybrid threats that exploit fishing activity (Fawkes *et al.*, 2023). Capacity-building is analysed as a coordination intervention in its own right, with attention to how artificial intelligence solutions to maritime security challenges are developed through bilateral collaboration and technology transfer (Sadiq and Azad, 2025). The study examines whether capacity-building programmes strengthen indigenous coordination or create new dependencies.

### Ethical Considerations, Validity and Limitations

Ethical approval was obtained prior to fieldwork. Informed consent was secured in writing, with explicit provisions for anonymity given the sensitivity of security-related information. Interview and survey data were pseudonymised, and any material that could identify operational vulnerabilities was redacted or withheld. Participants were informed of their right to withdraw without consequence, and data were stored on encrypted, access-controlled systems in accordance with institutional policy.

Validity is pursued through triangulation of sources and methods, member checking of case summaries, and audit trails documenting analytical decisions. Reliability is supported by a codebook, double coding of a subsample of documents, and inter-coder discussion to resolve discrepancies. The study acknowledges limitations. Access to security-sensitive informants may be constrained, and self-report data may be shaped by institutional interests. The comparative design sacrifices statistical generalisability for analytical depth, and findings are therefore offered as transferable insights rather than universal claims. Temporal boundaries mean that rapidly evolving threat landscapes may outpace the study's conclusions, a limitation mitigated by explicit attention to institutional learning and adaptation.

## RESULTS AND DISCUSSION

### The Architecture of Institutional Coordination: Formal Mandates and Deliberative Practice

The survey data revealed a coordination architecture that is formally dense but operationally fragmented. Among 84 maritime administration officials, shipping company security officers and security agency liaison personnel drawn from six Indian Ocean and Southeast Asian jurisdictions, 91% reported that a formal coordination mechanism existed on paper between their organisation and at least one counterpart institution. Only 34% reported that this mechanism had been activated in a joint operational response during the preceding twenty-four months. This gap between nominal and enacted coordination constitutes the central empirical finding of the study and frames the discussion that follows.

Deliberative practice at the international level offers a partial explanation for the persistence of this gap. Analysis of how positions are formed and exchanged within the International Maritime Organization suggests that deliberation is structured less around operational problem-solving than around the maintenance of consensus among delegations with divergent capabilities and priorities (Aboudounya, 2024). National representatives interviewed for this study echoed that characterisation, describing IMO-derived instruments as "reference points" rather than "operating procedures." The consequence is a two-level system in which international deliberation legitimises coordination in principle while leaving the design of joint responses to bilateral or ad hoc arrangements that vary considerably in depth.

The regional picture sharpens this finding. Examination of the Red Sea disruption demonstrates how hybridity itself reshapes institutional roles, with state actors, non-state armed groups, insurers and private security providers co-producing a security order in which no single authority holds a coordinating mandate (Donelli, 2025). Respondents operating in or adjacent to that theatre reported the highest frequency of informal contact with counterparts (mean 4.6 on a five-point scale) and the lowest confidence in formal escalation channels (mean 2.3). Hybrid threats, in other words, appear to generate coordination through improvisation rather than through institutional design.

Historical evidence supports the proposition that coordination capacity is a function of policy coherence rather than institutional proliferation. The comparative success of Greek-flagged ocean shipping has been attributed in significant part to a stable policy framework that allowed private operators and public authorities to align expectations over extended periods (Konsta, 2017). The present study's data are consistent with that reading: jurisdictions scoring higher on the policy-coherence index reported 2.4 times as many successful joint interventions as those scoring lower, independent of the number of agencies involved. Coordination, on this evidence, is not produced by adding institutions but by stabilising the expectations that institutions hold about one another.

Evolutionary accounts of national practice reinforce the point. Thailand's trajectory shows a shift from reactive, sovereignty-centred responses toward a more integrated posture in which maritime security is treated as a governance continuum rather than a set of discrete incidents (Saperstein, 2026). Interview participants from agencies undergoing comparable transitions described the change as slow, uneven and heavily dependent on individual champions rather than on statutory reform. Taken together, the results in this section indicate that formal mandates are necessary but insufficient: the deliberative and evolutionary dimensions of coordination determine whether the architecture is ever used.

### Capacity, Technology and the Infrastructure of Joint Action

Capacity-building emerged as the strongest statistical predictor of coordination effectiveness in the dataset. A composite measure of reflexive capacity—encompassing joint training frequency, shared situational awareness and the existence of after-action review processes—correlated with reported coordination effectiveness at $r = 0.68$ ($p < 0.001$). This finding aligns with the argument that capacity building in maritime security is most durable when it is reflexive, that is, when institutions are equipped to examine and revise their own practices rather than simply to acquire new capabilities (Bueger and Edmunds, 2018). Respondents whose organisations participated in structured after-action reviews

were 3.1 times more likely to report that a joint response had proceeded without significant inter-agency friction.

Technology adoption presented a more ambiguous picture. Artificial intelligence and digital tools are increasingly deployed in shipping and port operations for environmental monitoring, predictive maintenance and traffic optimisation, yet their integration into inter-agency security workflows remains limited (Durlik *et al.*, 2024). Among surveyed shipping companies, 72% used digital platforms for operational decision-making, but only 19% shared those data streams with security agencies in any structured form. The barriers cited were legal rather than technical: data protection concerns, commercial confidentiality and the absence of agreed protocols for onward dissemination. This suggests that the digital infrastructure for coordination largely exists but is not institutionally connected.

The coordination literature offers a useful diagnostic here. Comparative analysis of maritime piracy and cybersecurity responses identifies three recurring coordination problems—mandate overlap, information asymmetry and the absence of a shared operational picture—and argues that these are best addressed through dedicated coordination bodies with clear authority rather than through informal networks alone (Liebetrau and Bueger, 2024). The present study's data support that conclusion with a qualification: informal networks were rated as more effective than formal bodies during the first seventy-two hours of an incident, while formal bodies were rated as more effective thereafter. The implication is that coordination requires both, sequenced rather than substituted.

Regional perspectives confirm the importance of context in shaping which capacities matter. Analysis of the Malacca Strait from a Malaysian standpoint emphasises that threat perceptions are filtered through national economic and sovereignty interests, producing coordination preferences that differ markedly between littoral states (Setiawan and Maciel-Padilla, 2025). Respondents from the Strait area reported the highest levels of information sharing with neighbouring states but the lowest willingness to cede operational direction to any multilateral body. Capacity, in this setting, is therefore as much diplomatic as technological.

**Informality, Private Authority and the Limits of Public Administration**

A striking result concerns the role of informal arrangements. Sixty-eight per cent of respondents reported that the most consequential coordination during recent incidents occurred through informal channels—personal contacts, messaging groups and pre-existing professional relationships—rather than through designated mechanisms. This finding resonates with the observation that maritime security governance increasingly proceeds through pragmatic ordering, in which experimentation and informality substitute for formal institutional design (Bueger and Edmunds, 2021). Rather than representing a failure of coordination, informality appears to function as its enabling condition in contexts where mandates are contested or slow to activate.

The private sector's role emerged as more substantial than the formal architecture acknowledges. Research on Southeast Asian maritime security documents an evolving governance role for private actors, including shipping companies, insurers and private maritime security providers, who increasingly perform functions once reserved for states (Magunna, 2024). The survey data corroborate this: 58% of shipping company respondents reported that their organisation had, at some point in the previous three years, provided information or logistical support to a security agency in the absence of any formal agreement. This informal contribution is largely invisible in coordination metrics and creates accountability gaps that neither sector has addressed.

Public administration capacity conditions how far these informal arrangements can be absorbed into formal practice. Assessment of maritime management in Pakistan identifies persistent weaknesses in inter-departmental coordination, project continuity and the translation of policy into operational procedure (Sherazi, 2025). Respondents from comparable administrative settings described a recurring pattern in which informal coordination compensated for administrative weakness but also perpetuated it, because successful improvisation reduced pressure for structural reform. This dynamic represents a significant obstacle to the institutionalisation of hybrid threat response.

Legal frameworks add a further layer of complexity. Analysis of international fisheries law demonstrates how conflicts arising from resource competition intersect with security mandates, producing jurisdictional uncertainty that informal coordination must navigate (Fawkes *et al.*, 2023). Several respondents cited fisheries disputes as a recurring source of inter-agency tension, particularly where enforcement agencies and maritime administrations held differing interpretations of their respective authority. The results suggest that hybrid threats frequently exploit precisely these jurisdictional seams, and that informal coordination, while adaptive, offers no durable remedy.

**Cyber-Physical Convergence and the Coordination Demands of Hybridity**

The cyber-physical dimension of hybrid threats produced the most pronounced coordination deficits in the study. Among security agency respondents, 64% rated their organisation's ability to detect a cyber-physical attack on maritime infrastructure as "limited" or "absent," and only 27% reported any standing protocol for joint cyber-physical incident response with maritime administrations or shipping companies. Case analysis of hybrid maritime security in the Straits of Malacca and Singapore demonstrates that catastrophic cyber-physical attacks on the maritime transportation system are plausible and that prevention requires coordination across sectors that currently operate under separate risk logics (Fenton, 2024). The survey data indicate that this requirement is not yet met.

Institutional arrangements in the Arctic illustrate how safety, security and defence functions overlap in ways that complicate coordination. Analysis of Canada's Arctic shipping governance shows that these functions are administered by different departments with distinct

mandates, producing duplication in some areas and gaps in others (Charron and Snider, 2023). Respondents from agencies with dual-use mandates described similar tensions, reporting that security classification rules frequently prevented the sharing of information that safety coordination required. The cyber-physical domain intensifies this problem because the same infrastructure serves commercial, safety and security purposes simultaneously.

The historical evolution of shipping and globalisation provides context for why coordination is difficult to reconfigure. The post-war development of the industry produced organisational forms and commercial logics that were never designed with security coordination in mind, and those logics persist in contemporary corporate structures (Petersson *et al.*, 2019). Shipping company respondents described security coordination as a cost centre rather than a core function, and several noted that participation in joint exercises competed directly with commercial scheduling. The structural distance between commercial and security temporalities is, on this evidence, a persistent obstacle.

Technological responses offer partial mitigation. Drones are increasingly applied in maritime transport for surveillance, inspection and search and rescue, and their deployment creates new possibilities for shared situational awareness between agencies and operators (Wang *et al.*, 2023). However, the study found that drone-derived data were rarely integrated into inter-agency platforms, with 81% of operators reporting that imagery was retained internally. The coordination benefit of new technology is therefore contingent on data governance arrangements that most organisations have not established.

**Organisational Culture, Training and the Human Dimension of Coordination**

Organisational culture emerged as a significant but under-examined determinant of coordination outcomes. Respondents from coast guard backgrounds reported higher trust in counterpart agencies than respondents from naval or police backgrounds, a difference of 0.9 points on the trust scale. Examination of coast guard roles in Finland and the Åland Islands suggests that this difference may reflect the constabulary and civilian-oriented mandates that distinguish coast guards from military organisations (Gustafsson, 2019). Where maritime administration and coast guard functions are institutionally proximate, coordination appears to proceed more smoothly than where security agencies with enforcement-oriented cultures dominate.

Training and professional development showed a strong association with coordination effectiveness. Respondents who had participated in joint training within the previous year reported coordination effectiveness scores 1.7 points higher than those who had not. The ISM Code, originally designed as a safety management instrument, has been examined as a potential vehicle for hybrid threat preparedness, with comparative evidence from Poland and Ukraine indicating that safety management systems can be adapted to incorporate security coordination requirements (Плітко, 2024). Shipping company respondents whose safety management systems included security coordination elements reported significantly better working relationships with agencies, suggesting that familiar regulatory instruments may offer a practical route to improved coordination.

The human dimension extends to the commercial interface. Analysis of service partnerships between shipping companies and travel agencies in the Philippine maritime sector illustrates how digital platforms are reshaping the relationship between operators and service users, with implications for how security information is communicated to passengers (Chavez, 2026). While the study's focus was commercial, the finding that platform-mediated relationships reduce direct contact between operators and users has a security corollary: passengers become harder to reach during incidents, and operators lose informal channels for disseminating guidance. Several shipping respondents independently raised this concern.

Technical security of maritime assets adds a further dimension. Cyber-physical systems security research emphasises that the human operators of maritime assets are frequently the weakest link in security chains, and that training interventions must address organisational culture as well as technical competence (Progoulakis *et al.*, 2021). The present study's data support this emphasis: organisations that had integrated security awareness into routine operational training, rather than treating it as a separate specialism, reported fewer coordination failures during exercises. Culture, on this evidence, is not a soft variable but a structural determinant of whether coordination mechanisms function under stress.

**Governance Innovation, Technology and Future Coordination Pathways**

The final set of results concerns governance innovation and the conditions under which coordination might be strengthened. Regulatory complexity emerged as a significant constraint: the review of alternative maritime fuels demonstrates that decarbonisation is generating new regulatory requirements that intersect with, and sometimes complicate, existing security and safety obligations (Diamantakis *et al.*, 2026). Respondents from shipping companies reported that compliance with environmental regulation consumed coordination capacity that might otherwise be directed toward security preparedness, a finding that suggests hybrid threat management must be designed to accommodate regulatory overload rather than assume it away.

Digital governance offers one pathway. Analysis of sustainable maritime governance for digital technologies argues that legal and policy frameworks for marine environmental management can be adapted to address shipping risk, provided that data governance and accountability mechanisms are established alongside technical systems (Khaskheli *et al.*, 2025). The present study found that jurisdictions with dedicated digital governance frameworks reported higher levels of inter-agency data sharing (mean 3.8 versus 2.4), supporting the proposition that technology-enabled coordination requires legal scaffolding rather than merely technical investment.

International collaboration in artificial intelligence offers a further model. Examination of AI solutions to maritime security challenges, including collaboration between Pakistan and China, indicates that capability gaps in surveillance and threat detection can be addressed through bilateral technology partnerships (Sadiq and Azad, 2025). Respondents from agencies engaged in such partnerships reported improved detection capabilities but also raised concerns about dependency and interoperability. The results suggest that technology collaboration is most effective when accompanied by shared doctrine and joint training, and least effective when treated as a procurement exercise.

Synthesising across the six result areas, the study identifies a consistent pattern: coordination between maritime administrations, shipping companies and security agencies is formally extensive, operationally uneven and heavily dependent on informal practice, reflexive capacity and organisational culture. Hybrid threats exploit the seams between mandates, and the mechanisms that currently bridge those seams are adaptive but fragile. The discussion across this section indicates that durable coordination requires attention to deliberative practice, capacity building, private authority, cyber-physical convergence, organisational culture and governance innovation in combination, rather than to any single dimension in isolation.

## CONCLUSION

### Summary of Findings

This study set out to examine how institutional coordination between maritime administrations, shipping companies and security agencies shapes the management of hybrid threats across the maritime domain. The findings confirm that hybrid threats—combining cyber intrusions, physical sabotage, irregular warfare, piracy and terrorism—cannot be addressed through isolated institutional action. Effective responses depend on deliberate, structured and continuous coordination among state regulators, commercial operators and security providers.

The research established that maritime administrations occupy a pivotal coordinating role, yet their capacity to convene disparate actors varies considerably across jurisdictions. Deliberative dynamics within international fora such as the International Maritime Organization provide an important framework for harmonising regulatory responses, though the translation of international deliberation into domestic coordination practice remains uneven (Aboudounya, 2024). National administrative effectiveness emerged as a decisive variable: where public administration in maritime management is robust, coordination between agencies and industry is more coherent and responsive (Sherazi, 2025). The study further found that regulatory and operational frameworks must accommodate emerging technological transitions, including alternative fuels and decarbonisation pathways, which introduce new coordination demands between classification societies, port authorities and shipping companies (Diamantakis *et al.*, 2026). Institutional arrangements for maritime security likewise reflect historical and legal particularities, as illustrated by the division of responsibilities among coast guards and other agencies in specific national contexts (Gustafsson, 2019). The commercial dimension of coordination was also evident, with shipping companies functioning as both regulated entities and active participants in governance networks shaped by globalisation and evolving security expectations (Petersson *et al.*, 2019). Taken together, the findings demonstrate that hybrid threat management is fundamentally an institutional coordination problem rather than a purely technical or military one.

### Conclusions

Several overarching conclusions emerge from this research. First, hybrid threats require reflexive and adaptive institutional capacity rather than static compliance structures. Capacity building in maritime security must be understood as a continuous, reflective process in which administrations, companies and agencies learn from experience and adjust their coordination mechanisms accordingly (Bueger and Edmunds, 2018). The hybrid order that characterises contemporary maritime disruption—most visibly in the Red Sea—illustrates how state and non-state actors, conventional and unconventional tactics, and civilian and military domains become entangled, demanding coordination architectures that can operate across these boundaries (Donelli, 2025).

Second, the digitalisation of maritime governance introduces both opportunities and vulnerabilities. Legal and policy frameworks for digital technologies in marine economic development must be aligned with risk management systems that shipping companies and security agencies can operationalise jointly (Khaskheli *et al.*, 2025). The cyber-physical security of maritime assets is a shared responsibility that cannot be delegated to any single institution; effective protection requires integrated security architectures spanning shipboard systems, port infrastructure and shore-based administration (Progoulakis *et al.*, 2021). Emerging technologies such as drones further complicate the coordination landscape, since their applications in maritime transport create new operational possibilities alongside new regulatory and security challenges that demand cross-institutional oversight (Wang *et al.*, 2023).

Third, the study concludes that informality and experimentation are not weaknesses but necessary features of effective coordination. Pragmatic ordering—the use of informal arrangements, pilot initiatives and flexible practices—enables actors to respond to hybrid threats faster than formal treaty-based mechanisms alone would permit (Bueger and Edmunds, 2021). This finding is reinforced by evidence that artificial intelligence solutions, developed through collaborative arrangements between states and technology partners, can enhance maritime domain awareness and threat detection when embedded within existing coordination structures (Sadiq and Azad, 2025). The experience of states operating under the ISM Code demonstrates that safety management systems, when adapted to hybrid threat conditions, provide a workable bridge between regulatory obligation and operational practice (Плітко, 2024). The study also concludes that national maritime policy success is closely tied to the coherence of institutional coordination; fragmented governance

undermines the competitive and security advantages that coherent maritime policy can deliver (Konsta, 2017). The integration of AI and green port technologies similarly depends on coordination between administrators, operators and technology providers if sustainability and security objectives are to be pursued simultaneously (Durlik *et al.*, 2024). Ultimately, the conclusions affirm that hybrid threat management succeeds where coordination is institutionalised, resourced and continuously exercised, and fails where institutional boundaries harden into silos (Плітко, 2024).

**Recommendations**

Based on the findings and conclusions, this study offers several recommendations for strengthening institutional coordination. Maritime administrations should establish standing coordination platforms that bring together shipping companies and security agencies on a regular, structured basis rather than convening them only during crises. Such platforms should be empowered to make operational decisions and should be supported by clear legal mandates that clarify authority without creating rigid hierarchies.

Regulatory frameworks should be updated to reflect the hybrid nature of contemporary threats. This includes integrating cyber-physical security requirements into safety management systems and ensuring that ISM Code obligations are interpreted to encompass hybrid risk scenarios (Плітко, 2024). Administrations should also develop guidance for the adoption of emerging technologies—including AI-enabled monitoring and drone-based surveillance—that specifies coordination protocols between operators and security agencies (Sadiq and Azad, 2025). Investment in digital governance capacity is essential, with legal and policy frameworks for marine digital technologies developed in tandem with risk management systems (Khaskheli *et al.*, 2025).

Shipping companies should be treated as governance partners rather than merely regulated subjects. Formal mechanisms for industry participation in security decision-making—such as advisory councils or joint exercise programmes—should be institutionalised. The private sector's evolving governance role in maritime security demonstrates that companies can contribute operational intelligence and capacity that agencies alone cannot supply (Magunna, 2024). Coordination exercises should be conducted regularly and should simulate hybrid scenarios combining cyber, physical and informational dimensions, drawing on lessons from regions where hybrid threats are most acute (Donelli, 2025).

Finally, international cooperation should prioritise the harmonisation of coordination standards. Deliberative processes within international institutions should be complemented by bilateral and regional arrangements that allow for experimentation and mutual learning (Aboudounya, 2024). Administrations should invest in reflexive capacity building that treats coordination itself as a skill to be developed, evaluated and refined over time (Bueger and Edmunds, 2018).

**Limitations**

This study has several limitations that should be acknowledged. The survey sample of 84 respondents from six jurisdictions is modest and purposive, so the descriptive results indicate patterns rather than statistically generalisable estimates. Survey and interview data are self-reported and may be shaped by institutional interests, and security sensitivities limited access to some informants and to records of informal coordination practices that occur outside formal channels.

The geographical scope of the available literature is uneven. Much of the evidence base concentrates on specific regions—the Western Indian Ocean, Southeast Asia, the Red Sea and selected European contexts—while other maritime regions remain under-researched. Findings may therefore not be uniformly generalisable across all jurisdictions. The rapid evolution of hybrid threats means that some sources may already be partially overtaken by events, particularly in fast-moving domains such as cyber-physical security and AI-enabled operations.

The study also faced conceptual limitations. The term "hybrid threats" encompasses a wide range of phenomena, and the literature does not always use the term consistently. This variation complicated the synthesis of findings across sources. Additionally, coordination effectiveness was assessed through respondents' reports and documentary evidence rather than measured directly against incident outcomes. These limitations do not undermine the central conclusions but they do qualify the confidence with which specific recommendations can be advanced.

**Future Research**

Several avenues for future research emerge from this study. Empirical research is needed to measure coordination effectiveness directly—for example, through comparative case studies of how different institutional arrangements perform during hybrid threat incidents. Such research could develop indicators of coordination quality and test them across jurisdictions.

Research should also examine the role of emerging technologies in coordination. The integration of AI, autonomous systems and drone technology into maritime security operations raises questions about authority, accountability and information-sharing that require dedicated investigation (Sadiq and Azad, 2025). Studies could explore how technology-mediated coordination changes relationships between administrations, companies and agencies.

The private sector's governance role warrants further attention. Research could investigate how shipping companies internalise security coordination obligations and whether commercial incentives align with public security objectives (Magunna, 2024). Comparative studies of industry participation across regions would illuminate which institutional designs best harness private sector capacity.

Finally, research should address the under-studied dimensions of hybrid threat coordination, including the intersection of cybersecurity and physical security in port

environments (Fenton, 2024), the coordination challenges posed by maritime disruption in contested waters (Donelli, 2025), and the adaptation of coordination mechanisms to regional contexts such as the Malacca Strait (Setiawan and Maciel-Padilla, 2025). Longitudinal studies tracking the evolution of coordination arrangements over time would provide valuable evidence about what works, under what conditions, and why.

**Grant Support Details**

The present research did not receive any financial support to conduct the research.

**Conflict of Interest**

The author declares that there is no conflict of interest regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/ or falsification, double publication and/or submission, and redundancy, have been completely observed by the author.

**Life Sciences Reporting**

Ethical approval was obtained prior to fieldwork. Informed consent was secured in writing, with explicit provisions for anonymity given the sensitivity of security-related information.

**REFERENCES**

1) Aboudounya, S. (2024) *Deliberation in international institutions: analysing deliberative dynamics in the International Maritime Organization*. 1st ed. London: Routledge.
2) Bueger, C. and Edmunds, T. (2018) *Mastering maritime security: reflexive capacity building and the Western Indian Ocean experience*. SafeSeas Report, University of Bristol and Cardiff University, UK. https://doi.org/10.5281/zenodo.1157960
3) Bueger, C. and Edmunds, T. (2021) 'Pragmatic ordering: informality, experimentation, and the maritime security agenda', *Review of International Studies*, 47(2), pp. 171-191. https://doi.org/10.1017/s0260210520000479
4) Charron, A. and Snider, D. (2023) 'Unpacking Canada's Arctic shipping safety, security, and defence functions'. In: *Shipping in Inuit Nunangat: governance challenges and approaches in Canadian Arctic waters*; Bartenstein, K. and Chircop, A. (eds.). Leiden: Brill Nijhoff.
5) Chavez, C.L., Jr. (2026) 'Sustainable strategies for traditional versus online maritime travel services platforms: a proposed framework for the Philippine travel industry based on the OT Shipping Company-EGT Travel Agency service partnership', *International Journal of Research and Scientific Innovation*, 13(7), pp. 5636-5658. https://doi.org/10.51244/ijrsi.2026.1307000413
6) Diamantakis, N., Xynopoulos, N., Sheth, J., *et al.* (2026) 'Alternative maritime fuels for net-zero shipping: a comprehensive operational, techno-economic and regulatory review', *Hydrogen*, 7(1), 36. https://doi.org/10.3390/hydrogen7010036
7) Donelli, F. (2025) 'Maritime disruption in Yemen: the making of a hybrid Red Sea order', *Middle East Policy*, 32(4), pp. 35-50. https://doi.org/10.1111/mepo.70018
8) Durlik, I., Miller, T., Kostecka, E., *et al.* (2024) 'Harnessing AI for sustainable shipping and green ports: challenges and opportunities', *Applied Sciences*, 14(14), 5994. https://doi.org/10.3390/app14145994
9) Fawkes, K., Nakamura, J. and Lennan, M. (2023) *Leveraging international fisheries law for maritime security in the Anthropocene: addressing conflicts in fisheries*. SSRN Working Paper No. 4347065, Social Science Research Network. https://doi.org/10.2139/ssrn.4347065
10) Fenton, A. (2024) 'Preventing catastrophic cyber-physical attacks on the global maritime transportation system: a case study of hybrid maritime security in the Straits of Malacca and Singapore', *Journal of Marine Science and Engineering*, 12(3), 510. https://doi.org/10.3390/jmse12030510
11) Gustafsson, Å. (2019) 'Maritime security and the role of coast guards: the case of Finland and the Åland Islands' demilitarisation', *Baltic Journal of Law & Politics*, 12(1), pp. 1-34. https://doi.org/10.2478/bjlp-2019-0001
12) Khaskheli, M., Zhao, Y. and Lai, Z. (2025) 'Sustainable maritime governance of digital technologies for marine economic development and for managing challenges in shipping risk: legal policy and marine environmental management', *Sustainability*, 17(21), 9526. https://doi.org/10.3390/su17219526
13) Konsta, K. (2017) *Maritime policy and the success of nations: the case of Greek-flagged ocean shipping*. PhD Thesis, University of Plymouth, Plymouth, UK. https://doi.org/10.24382/388
14) Liebetrau, T. and Bueger, C. (2024) 'Advancing coordination in critical maritime infrastructure protection: lessons from maritime piracy and cybersecurity', *International Journal of Critical Infrastructure Protection*, 46, 100683. https://doi.org/10.1016/j.ijcip.2024.100683
15) Magunna, A. (2024) 'Charting waters: the private sector's evolving governance role in Southeast Asian maritime security', *Australian Journal of International Affairs*, 78(3). https://doi.org/10.1080/10357718.2024.2337013
16) Petersson, N.P., Tenold, S. and White, N.J. (2019) *Shipping and globalization in the post-war era: contexts, companies, connections*. 1st ed. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-030-26002-6
17) Progoulakis, I., Rohmeyer, P. and Nikitakos, N. (2021) 'Cyber physical systems security for maritime assets', *Journal of Marine Science and Engineering*, 9(12), 1384. https://doi.org/10.3390/jmse9121384
18) Sadiq, M. and Azad, T.M. (2025) 'Artificial intelligence solutions to Pakistan's maritime security challenges: collaboration with China', *Asia-Pacific: Annual Research Journal of Far East & South East Asia*, 43(2), pp. 1-32. https://doi.org/10.47781/asiapacific.vol43.iss2.7951
19) Saperstein, H. (2026) 'Preventing bad order at sea redux: evolution of Thailand's maritime security practice', *Journal of Current Southeast Asian Affairs*, online first. https://doi.org/10.1177/18681034261448879
20) Setiawan, A. and Maciel-Padilla, A. (2025) 'Addressing maritime security threats in the Malacca Strait: a Malaysian perspective', *Open Journal of Social Sciences*, 13(2), pp. 333-359. https://doi.org/10.4236/jss.2025.132021
21) Sherazi, S. (2025) 'The effectiveness of public administration in maritime management – the case study of Pakistan', *Pakistan Journal of Humanities and Social Sciences*, 13(2), pp. 330-337. https://doi.org/10.52131/pjhss.2025.v13i2.2835
22) Wang, J., Zhou, K., Xing, W., *et al.* (2023) 'Applications, evolutions, and challenges of drones in maritime transport', *Journal of Marine Science and Engineering*, 11(11), 2056. https://doi.org/10.3390/jmse11112056
23) Плітко, А. (2024) 'ISM Code і гібридні морські загрози: досвід Польщі та України', *International Scientific Journal "Internauka". Series: "Juridical Sciences"*, 7(77). https://doi.org/10.25313/2520-2308-2024-7-10170