

Governing Cross-Border Cyber Threat Intelligence Sharing for Maritime Security Resilience in the Strait of Malacca

Suhirwan^{1*}

¹Department of Asymmetric Warfare, Universitas Pertahanan Republik Indonesia, Indonesia

*Corresponding Author Email: suhirwan@idu.ac.id

Received: 2 February 2026; Revised: 5 April 2026; Accepted: 11 April 2026

Abstract

The Straits of Malacca and Singapore are among the most strategically important maritime chokepoints in the global trading system. Although conventional threats such as piracy have been managed through regional cooperation, the rapid digitalisation of ports, vessel traffic systems, and naval command infrastructures has created new hybrid cyber-physical vulnerabilities. Despite recurring cyber incidents between 2020 and 2025, no institutionalised real-time cross-border Cyber Threat Intelligence (CTI) mechanism has emerged among Indonesia, Malaysia, and Singapore. This study examines the puzzle of institutional inertia under growing threat interdependence and its implications for SDG 9, Target 9.1 on resilient infrastructure, and SDG 17, Targets 17.16 and 17.17 on knowledge-sharing and effective public-private partnerships. Drawing on 18 semi-structured interviews and qualitative analysis of policy documents from 2020 to 2025, the study identifies three governance bottlenecks: legal-institutional ambiguity, sovereignty-related political constraints, and technical-operational interoperability gaps. Building on Regional Security Complex Theory and regime complexity scholarship, the article theorises Cooperative Sovereignty as a middle-ground governance modality between supranational integration and sovereignty-maximising bilateralism. It proposes the Malacca Cyber Intelligence Node (MCIN) as a federated, sovereignty-compatible mechanism for structured cyber threat signalling while preserving national control over data. The study contributes to governance scholarship and offers actionable pathways for strengthening maritime cyber resilience in sovereignty-sensitive regions.

Keywords: Cooperative Sovereignty; Cyber Threat Intelligence; Maritime Cyber Resilience; Regional Governance

Copyright © 2026 by the Author. Published by the Pusat Penelitian Ilmu Sosial dan Humaniora Kontemporer, Indonesia. This is an open access article distributed under the terms of the CC BY-SA Licence (<https://creativecommons.org/licenses/by-sa/4.0>).

How to Cite: Suhirwan, S. (2026). Governing Cross-Border Cyber Threat Intelligence Sharing for Maritime Security Resilience in the Strait of Malacca. *Journal of Contemporary Governance and Public Policy*, 7(1), 107-134. <https://doi.org/10.46507/jcgpp.v7i1.797>

Permalink/DOI: <https://doi.org/10.46507/jcgpp.v7i1.797>

Introduction

The Straits of Malacca and Singapore constitute one of the most strategically vital maritime chokepoints in the global economy, serving as the shortest sea route between the Indian and Pacific Oceans and carrying a substantial share of global trade and energy flows, particularly for Northeast Asia (Qu & Meng, 2012; Rusli et al., 2021). Their dense traffic concentration and deep integration into regional supply chains make them indispensable, yet structurally vulnerable (Fenton, 2024; Tuan Binh et al., 2022). In recent years, however, the nature of that vulnerability has changed. The rapid digitalisation of port logistics systems, vessel traffic management platforms, automated container handling, and naval command infrastructures has expanded the attack surface of maritime governance. Maritime security is no longer confined to physical patrols and territorial surveillance; it now operates within a hybrid cyber-physical ecosystem characterised by complex interdependencies and cascading risks (de la Peña Zarzuelo, 2021; Weaver et al., 2022).

Between 2020 and 2025, several cyber-related incidents reflected this structural shift. Ransomware attacks temporarily disrupted container operations at major regional ports, generating ripple effects across logistics networks. These incidents demonstrate the emergence of hybrid cyber-maritime threats affecting navigation systems, port operations, and naval infrastructures (Louart et al., 2023; Soner et al., 2024). Rather than isolated anomalies, they indicate an evolving threat environment in which contemporary maritime insecurity increasingly exploits jurisdictional gaps between cyber agencies and maritime authorities.

Despite rising digital exposure, governance adaptation has lagged behind threat evolution. Indonesia, Malaysia, and Singapore maintain established cooperative frameworks such as the Malacca Strait Patrols (MSP) and the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia Information Sharing Centre (ReCAAP ISC) (Bolbot et al., 2022; Poonnawatt, 2023), but these remain primarily oriented towards conventional maritime security (Caballero-Anthony, 2020). No institutionalised, real-time cross-border cyber threat intelligence (CTI) mechanism exists among the littoral states. Intelligence sharing related to cyber threats continues to rely mainly on national channels and informal coordination, limiting regional responsiveness in a highly interdependent maritime corridor.

This institutional lag creates a broader governance challenge. Maritime cyber disruptions undermine infrastructure reliability and supply chain continuity, both of which are central to sustainable development and regional resilience (Jin et al., 2024). Yet cooperative reform must operate within ASEAN's consensus-based and sovereignty-sensitive normative order (Rosnani et al., 2022). The governance question is therefore not merely technological but institutional: how can structured cross-border cyber intelligence exchange emerge within a framework that prioritises non-interference?

Existing scholarship offers only partial insights. Regional security complex theory explains dense threat interdependence (Buzan & Wæver, 2003), while empirical studies of Southeast Asian governance highlight institutional layering and fragmentation

(Fortnam et al., 2022). These analyses illuminate fragmentation, but they do not fully explain why repeated cyber escalation has failed to catalyse structured intelligence-sharing mechanisms.

Parallel research in maritime cybersecurity documents increasing technical vulnerabilities in smart ports, navigation technologies, and maritime digital infrastructures (Androjna et al., 2021; Soner, 2025). While these studies advance understanding of hybrid cyber-physical risks, they prioritise technological mitigation over institutional design. As a result, vulnerability has been extensively mapped, but governance innovation remains under-theorised.

A third strand of literature examines cyber sovereignty and cross-border data governance in emerging economies. Scholars argue that Global South states increasingly treat data flows as strategic assets, thereby reinforcing localisation policies and non-interference principles (Horst et al., 2024; Pestana & Sofou, 2024). Comparative discussions often contrast this sovereignty-first orientation with European Union cybersecurity integration under binding regulatory frameworks (Aaronson & Leblond, 2018). However, the assumption that effective cyber cooperation requires sovereignty pooling does not translate easily to ASEAN's normative context, where non-interference is foundational rather than negotiable (Qiao-Franco et al., 2025).

Taken together, these strands of literature explain threat interdependence, regime complexity, and sovereignty sensitivity. Yet none systematically theorises a governance modality capable of reconciling real-time CTI exchange with deeply embedded non-interference norms (Chen & Gao, 2024). The persistent framing of sovereignty as an obstacle to cooperation obscures the possibility that institutional innovation may depend on recalibrating, rather than eroding, sovereign authority.

This study advances the concept of Cooperative Sovereignty as an intermediate governance modality situated between supranational integration and sovereignty-maximising bilateralism. Unlike supranational models, which pool authority through binding legal harmonisation, and unlike bilateral exchanges, which preserve sovereignty but limit scalability, Cooperative Sovereignty represents a calibrated institutional design (Montfort et al., 2023; Panke & Stapel, 2024). It preserves national control over sensitive cyber data while institutionalising structured, rule-based cross-border intelligence signalling. In this formulation, sovereignty becomes a relational capacity coordinated through procedural interoperability rather than authority transfer.

As summarised in Table 1, existing institutional arrangements in the Malacca Strait reveal an adaptation gap between traditional maritime security mandates and emerging cyber threat environments. Although mechanisms such as the Malacca Strait Patrols (MSP) and ReCAAP ISC provide effective coordination against conventional maritime threats, none currently incorporates operational cyber threat intelligence integration.

Table 1 illustrates the institutional adaptation gap characterising maritime governance in the Malacca Strait, where existing cooperative frameworks remain anchored in conventional security paradigms and have yet to operationalise cyber threat intelligence coordination. This institutional misalignment provides the empirical basis for examining why intensified hybrid threats have not translated into adaptive

governance reform. From an institutional evolution perspective, intensified hybrid threats should stimulate adaptive governance responses. Yet despite recurring incidents and growing digital interconnectivity, no structured regional CTI architecture has emerged among Indonesia, Malaysia, and Singapore (Triwahyuni et al., 2025). This divergence between threat escalation and institutional adaptation constitutes the study's central empirical puzzle. It suggests that structural and normative constraints, rather than capacity deficits alone, shape the trajectory of maritime cyber governance.

Table 1. Institutional Adaptation Gap in the Malacca Strait
Source: Adapted from Caballero-Anthony (2020) and Tenny and Kassim (2025)

Institution	Primary Mandate	Cyber Coverage	Governance Limitation
MSP	Coordinated maritime patrol	Physical maritime threats	No cyber intelligence protocol
ReCAAP ISC	Anti-piracy information sharing	Maritime crime reporting	No real-time CTI integration
ASEAN Cyber Mechanisms	Regional digital cooperation	Normative cybersecurity dialogue	Non-binding and lacking operational interoperability

To conceptualise a way forward, this study puts forward the Malacca Cyber Intelligence Node (MCIN), a federated coordination mechanism grounded in Cooperative Sovereignty. To clarify the theoretical positioning of Cooperative Sovereignty, Table 2 compares it with existing governance models in terms of sovereignty treatment, institutional depth, and scalability. The comparison shows that Cooperative Sovereignty offers a middle-path governance arrangement between the need for coordination and the desire to preserve state autonomy.

Table 2. Conceptual Positioning of Cooperative Sovereignty
Source: Author's synthesis based on Cui (2025)

Governance Model	Sovereignty Treatment	Institutional Depth	Scalability
Supranational integration	Sovereignty pooling	High	High
Bilateral intelligence sharing	Sovereignty maximization	Low	Low
Cooperative sovereignty	Sovereignty coordination	Medium	Medium-High

As illustrated in Table 2, Cooperative Sovereignty represents an intermediate mode of governance between supranational integration and bilateral intelligence sharing, enabling joint action without requiring sovereignty pooling. This framing also clarifies how cooperative arrangements may adapt more effectively to politically sensitive and strategically contested maritime spaces.

This middle-path positioning provides the conceptual foundation for proposing a federated coordination mechanism capable of operationalising sovereignty-compatible cyber intelligence exchange. The empirical investigation draws on 18 semi-structured interviews with maritime, cyber, and policy stakeholders across the three littoral states, complemented by policy document analysis covering the period 2020 to 2025. The study addresses two research questions: (1) What institutional, legal, and technological constraints impede real-time cross-border CTI exchange? and (2) How can a sovereignty-compatible governance architecture enhance operational resilience without contravening ASEAN's non-interference norm?

The article contributes in three ways. Theoretically, it develops Cooperative Sovereignty as a middle-ground institutional modality for cyber governance in sovereignty-sensitive regional orders. Empirically, it maps the governance bottlenecks that limit cross-border maritime CTI institutionalisation. Practically, it advances MCIN as a scalable coordination design for hybrid maritime resilience.

By shifting analytical emphasis from descriptive fragmentation to institutional design under normative constraint, this study offers a governance-oriented framework for strengthening maritime cyber resilience in regions where shared vulnerability coexists with strong sovereignty commitments.

Building on the preceding conceptual discussion, Figure 1 presents the Cooperative Sovereignty governance framework, integrating institutional mandates, intelligence coordination processes, and sovereignty management dynamics into a unified analytical model.

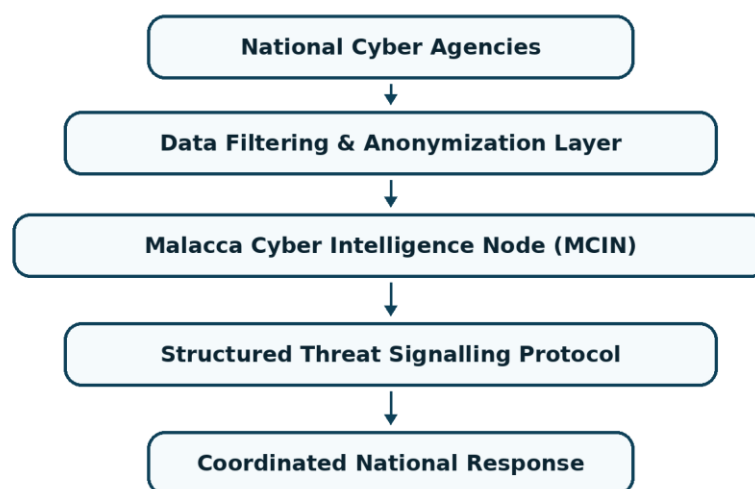


Figure 1. Cooperative Sovereignty Governance Framework
Source: Developed from Emerson et al. (2012) and Ishkhanyan (2025)

The framework visualises how cross-border cyber intelligence cooperation emerges through iterative interaction between the preservation of national authority and procedural interoperability, thereby forming the analytical lens that guides the empirical investigation. Together, Tables 1 and 2 and Figure 1 form an integrated analytical sequence linking empirical observation, theoretical positioning, and governance modelling, which structures the subsequent empirical analysis.

Research Methods

Guided by the Cooperative Sovereignty framework, this study adopted a qualitative governance design to examine institutional barriers to maritime cyber threat intelligence (CTI) sharing in the Malacca Strait. Specifically, the study combined document analysis and semi-structured interviews to investigate institutional mandates and coordination mechanisms relevant to cross-border governance in the cyber and maritime domains (Liebetrau & Bueger, 2024; Xu & Zuo, 2026). The documentary dataset comprised 47 regional policy documents published between 2020 and 2025, drawn from ASEAN institutions, national cybersecurity agencies, and maritime authorities. Integrating policy-level analysis with practitioner perspectives enabled empirical triangulation across institutional settings (Denzin, 1978; Flick, 2022). This methodological approach is consistent with qualitative security governance research that emphasises institutional process tracing and interpretive analysis (Caballero-Anthony, 2020; Fenton, 2024).

The document analysis covered national cyber strategies, regional cybersecurity frameworks, incident reports, and maritime cybersecurity guidelines. These included Indonesia's National Cyber Strategy 2020 to 2024, Singapore's Safer Cyberspace Masterplan 2023, the ASEAN Cybersecurity Cooperation Strategy 2021 to 2025, incident reports issued by Badan Keamanan Laut Republik Indonesia (Indonesian Maritime Security Agency, BAKAMLA), the Royal Malaysian Navy Maritime Command (RMN Maritime Command), and the Maritime and Port Authority of Singapore (MPA) between 2020 and 2025, as well as maritime cybersecurity guidelines issued by the International Maritime Organization (IMO). Documents were coded in NVivo 14 for themes related to sovereignty, data sharing, and interoperability within cyber-maritime governance regimes (Dhakal, 2022). To strengthen transparency, document selection followed a structured and explicit screening process consistent with qualitative trustworthiness criteria (Nowell et al., 2017) and informed by the logic of transparent identification and inclusion associated with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework (Moher et al., 2009).

Semi-structured interviews were conducted with a purposive sample of 18 stakeholders with direct operational experience of maritime cyber incidents. The sample comprised participants from Indonesia (n = 7), Malaysia (n = 6), and Singapore (n = 5), including cyber analysts, intelligence personnel, cybersecurity officials, and maritime security managers. Standardised participant codes reflected country representation, namely ID-01 to ID-07, MY-01 to MY-06, and SG-01 to SG-05, and supported consistent reporting while preserving anonymity. Participants were selected on the basis of their

functional relevance, decision-making authority, and or prior involvement in cross-border cyber incident responses (Abdullah et al., 2025). All participants provided informed consent. Interviews lasted between 45 and 75 minutes, were audio-recorded, transcribed verbatim, and supplemented by field notes capturing contextual observations and non-verbal cues.

Data analysis followed the six-phase thematic analysis framework developed by Braun and Clarke (2019) and further operationalised in applied qualitative security research (Naeem et al., 2023). The process involved repeated reading of transcripts for familiarisation, initial open coding in NVivo 14, generation of 142 descriptive codes such as “classification mismatch” and “delayed notification”, iterative clustering of codes into broader analytical themes such as “institutional fragmentation” and “sovereignty concerns”, review of themes through peer debriefing with two co-researchers, and final theme definition and refinement. Interview coding was used to identify recurring institutional, legal, and technological constraints affecting real-time cross-border CTI exchange. Quantitative expressions reported in the findings were operationalised through systematic coding and aggregation of qualitative interview data, thereby supporting analytical consistency while preserving interpretive depth.

To enhance methodological transparency, the study maintained an audit trail of key analytical decisions and conducted member checks by sharing preliminary findings with six participants for validation. Visual materials were developed using Microsoft Excel and related visualisation tools, while Microsoft Excel 365 was also used to generate descriptive statistics on incident frequency trends.

Ethical approval was granted by the Institutional Review Board of Universitas Pertahanan Republik Indonesia (reference: UD-IRB/2025/087). Participants received clear information regarding the aims of the research, data-use procedures, and their right to withdraw without penalty. All identifiable information was anonymised using country-prefixed codes, and institutional names were reported only where they were already publicly available. Data were stored in accordance with Undang-Undang Perlindungan Data Pribadi (Personal Data Protection Law), No. 27/2022, using AES-256 encrypted storage accessible only to the core research team.

Results and Discussion

Guided by the Cooperative Sovereignty governance framework presented in Figure 1, this section analyses the empirical findings across institutional, operational, and governance dimensions to explain how cross-border cyber threat intelligence exchange is constrained and how sovereignty-compatible cooperation may emerge.

To address the study’s two main research questions, this section presents and critically evaluates empirical findings drawn from 18 stakeholder interviews and 47 policy documents published between 2020 and 2025: (1) What technological, institutional, and legal obstacles impede the exchange of real-time cyber threat data among the littoral states of the Malacca Strait? and (2) How can operational resilience be strengthened while upholding sovereignty principles within an intelligence-sharing

MCIN governance architecture (Radanliev, 2025) compatible with ASEAN norms? Informed by Regional Security Complex Theory and aligned with the imperatives of the Sustainable Development Goals (SDGs), the analysis moves beyond descriptive fragmentation to identify systemic governance weaknesses and develop workable, collaborative solutions.

The Governance Paradox and SDG Imperatives

This subsection corresponds to the structural-context layer of the governance framework and examines how systemic dependence on the Malacca Strait contrasts with fragmented cyber governance responses. The Malacca Strait exemplifies a critical paradox of twenty-first-century maritime governance: although its strategic density, with more than 94,000 vessel transits annually, requires real-time cyber resilience to support Sustainable Development Goal (SDG) Target 9.1, namely to “develop quality, reliable, sustainable infrastructure”, institutional responses remain fragmented and delayed. The empirical findings indicate that cross-border cyber threat intelligence (CTI) exchange frequently exceeds the 72-hour threshold considered critical for supply chain reliability (Unctad, 2020), thereby undermining the operational logic of SDG Target 9.1. This delay stems less from technological incapacity than from institutional fragmentation, as cyber and maritime sectors continue to operate in parallel silos across Indonesia, Malaysia, and Singapore.

As one Indonesian cyber analyst stated, “We detect AIS spoofing near Batam within minutes, but getting approval to share indicators of compromise with Singapore takes three days” (ID-07). Such disconnects jeopardise port continuity and intensify risks associated with SDG Target 14.1, as delayed threat correlation may hinder timely responses to cyber-compromised ballast water or oil terminal systems, with potentially serious ecological consequences. This gap reveals a broader governance limitation in transforming shared vulnerability into collective resilience.

Empirical findings derived from 18 semi-structured interviews and a systematic review of 47 policy documents published between 2020 and 2025 indicate that formal regional mechanisms, such as the ReCAAP Information Sharing Centre (ISC) and the Malacca Straits Patrols (MSP), operate without clear cyber mandates, standardised incident taxonomies, or interoperable technical protocols for cyber-maritime threats (Edwards, 2022; Fenton, 2024). These institutions were originally established to address kinetic threats such as piracy and armed robbery, and their governance structures have not evolved sufficiently to reflect the hybrid character of contemporary maritime security challenges. As a result, the littoral states continue to address emerging cyber threats through ad hoc and informal arrangements.

In practice, this has led to the use of commercial encrypted messaging services such as WhatsApp and military-to-military hotlines to exchange indicators of compromise during crises (Magunna, 2024). Despite their immediacy, these channels are not institutionally scalable, auditable, or inclusive. They tend to exclude civilian cyber agencies such as Malaysia’s National Cyber Security Agency (NACSA) and Badan Siber dan Sandi Negara (National Cyber and Crypto Agency, BSSN) of Indonesia (Melaku, 2023).

One notable example was the 2023 Batam port ransomware incident, in which Badan Siber dan Sandi Negara (National Cyber and Crypto Agency, BSSN) identified malicious code within hours but was unable to notify Badan Keamanan Laut Republik Indonesia (Indonesian Maritime Security Agency, BAKAMLA) formally because of a classification mismatch: BSSN categorised the threat as “Confidential”, whereas BAKAMLA required “Secret” clearance for maritime alerts (ID-05).

Similarly, port operators at Tanjung Priok and Port Klang reported monthly detections of AIS spoofing attempts, yet lacked secure and legally protected channels through which to report them to national authorities because of concerns over liability exposure and commercial confidentiality (SG-05). Thus, although high-fidelity threat intelligence exists, it remains fragmented within separate institutional or private-sector domains and cannot easily contribute to a coherent regional defence posture. This operational reality highlights a wider systemic deficit (Afenyo & Caesar, 2023; Sharma, 2024).

Unlike the European Union’s top-down legal harmonisation under the NIS2 Directive (European Commission, 2025; Sałek & Fajdek, 2025), ASEAN states operate within a Cooperative Sovereignty framework that prioritises sovereignty, non-interference, and consensus, principles that are not easily aligned with binding cyber intelligence protocols. This governance gap reflects a broader challenge in the Global South. As noted by Edwards (2022), the “ASEAN Way” may produce institutional fragmentation without functional redundancy, while overlapping forums generate procedural activity without sufficient operational coherence (Bettani & Ahmed, 2023). Consequently, littoral states remain embedded in reactive bilateralism, which is insufficient to address transnational adversaries that deliberately exploit jurisdictional gaps among Singapore, Malaysia, and Indonesia (Fenton, 2024).

The result is a self-reinforcing cycle of limited cooperation: legal constraints legitimise technical minimalism, while political mistrust reinforces legal rigidity. Indonesia’s Undang-Undang Perlindungan Data Pribadi (Personal Data Protection Law), No. 27/2022, for example, restricts the cross-border sharing of “critical infrastructure” data without ministerial approval. Agencies therefore continue to use unstructured formats, such as PDF reports or email alerts, rather than machine-readable standards such as STIX/TAXII, resulting in six to eight hours of manual re-keying during joint threat assessments (Abraham et al., 2025). This immobility is institutional rather than technological, and reflects risk-averse organisational cultures that associate data sharing with strategic vulnerability rather than collective security (Subramaniam & Fernandez, 2025).

Importantly, this fragmentation also weakens progress towards SDG Targets 17.16 and 17.17, which emphasise knowledge-sharing partnerships and effective public-private collaboration. Port operators, who are often the first to detect cyber anomalies such as AIS spoofing or ransomware precursors, frequently withhold threat intelligence because of concerns over economic confidentiality and the absence of “good faith” liability protections (Magunna, 2024; Soner et al., 2024). As one port manager in Singapore explained, “Reporting threats risks exposing our security gaps to competitors”

(SG-03). This public-private divide keeps high-value threat data outside formal response loops, weakens regional situational awareness, and limits the development of inclusive, multi-stakeholder resilience.

In contrast to the Baltic Sea model, where European Union membership enables legal interoperability and standardised cyber-maritime exercises (Agastia, 2021; X. Chen & Yang, 2022), Southeast Asia requires sovereignty-sensitive governance innovation that respects ASEAN norms while enabling functional cooperation. This calls for a reconceptualisation of cyber sovereignty as a relational capability rather than a purely unilateral authority. Such a shift may be advanced through anonymised data pools, trusted intermediaries such as ReCAAP ISC, and confidence-building measures including collaborative tabletop exercises under the ASEAN Defence Ministers' Meeting-Plus (ADMM-Plus) framework (Lawale & Ahmad, 2025). Without such a shift, the Malacca Strait is likely to remain exposed to low-cost, high-impact hybrid operations, a systemic risk that sits uneasily with the SDG vision of cooperative, sustainable, and resilient infrastructure.

The persistence of delayed intelligence exchange despite shared vulnerability thus establishes the foundational governance paradox that shapes the subsequent institutional and operational constraints analysed in this study.

Institutional Fragmentation: Silos Within and Across Borders

Building on the governance paradox identified above, this subsection examines the institutional layer of the framework by analysing how national cyber-maritime governance architectures shape intelligence-sharing capacity.

The Malacca Strait littoral states exhibit significant differences in their national cyber-maritime governance architectures. Indonesia displays the highest degree of institutional fragmentation, with three key entities, Badan Siber dan Sandi Negara (National Cyber and Crypto Agency, BSSN), Badan Keamanan Laut Republik Indonesia (Indonesian Maritime Security Agency, BAKAMLA), and the Ministry of Defence, operating under separate legal mandates, reporting hierarchies, and classification standards. This structural compartmentalisation significantly constrains real-time information sharing (Chen et al., 2023; Huang et al., 2024). During the 2023 Batam port ransomware incident, BSSN identified malicious code within hours but was unable to notify BAKAMLA formally because of a classification mismatch: BSSN classified the threat as "Confidential", whereas BAKAMLA required "Secret" clearance for maritime alerts (ID-05). This finding is consistent with broader observations of institutional fragmentation in Southeast Asia (Bettani & Ahmed, 2023).

By contrast, Malaysia's governance architecture shows a greater degree of integration under the National Cyber Security Agency (NACSA), which coordinates civilian cyber policy at the national level. However, the Royal Malaysian Navy (RMN) Maritime Command maintains separate cyber units with incompatible threat databases and distinct communication channels, preventing automatic correlation during joint maritime operations (Magunna, 2024). This civil-military divide reduces situational

awareness during hybrid crises that cut across both domains (Tikanmäki & Ruoslahti, 2024).

Singapore demonstrates the highest level of institutional integration, with the Cyber Security Agency of Singapore (CSA), the Maritime and Port Authority of Singapore (MPA), and the Ministry of Defence (MINDEF) operating through unified protocols, standardised data formats, and shared threat-assessment procedures. This enables sub-hour cyber-maritime handovers during active incidents (Khan, 2024). Despite these national differences, all three countries face the same regional constraint: the absence of a legally binding, cyber-capable multilateral governance arrangement able to bridge institutional silos across borders (Edwards, 2022).

This fragmentation persists and intensifies at the regional level. Existing ASEAN mechanisms, such as the Malacca Straits Patrols (MSP) and the Expanded ASEAN Maritime Forum (EAMF), were originally designed to address kinetic threats such as piracy and armed robbery. They do not include cyber mandates, technical interoperability standards, or standardised taxonomies for hybrid cyber-physical incidents (Edwards, 2022). As a result, these institutions remain poorly equipped to respond to evolving maritime threat landscapes shaped by ransomware, AIS spoofing, and supply-chain intrusion.

As Edwards (2022) argues, this institutional structure produces “fragmentation without functional redundancy”: overlapping forums generate procedural activity but provide no fail-safe capacities for cyber-maritime contingencies. A telling example emerged during the 2024 Tri-Border Area cyber-smuggling operation, when Indonesian authorities intercepted encrypted communications but were unable to share decryption keys with Malaysian counterparts because no mutual legal assistance treaties (MLATs) for cybercrime were in place. This legal gap is not incidental; rather, it reflects a structural feature of ASEAN’s sovereignty-first orientation.

This institutional vacuum runs counter to SDG 17.16, which calls for enhanced partnerships in knowledge-sharing, and demonstrates that operational resilience is shaped as much by governance design as by threat awareness. Unlike the Baltic Sea model, where European Union membership enables legal harmonisation, joint cyber exercises, and cross-border data flows under arrangements such as the NIS2 Directive (Lawale & Ahmad, 2025), Southeast Asia continues to operate through the “ASEAN Way”, a normative order grounded in sovereignty, non-interference, and consensus-based decision-making (Dang & Mon, 2023; Honrada & Bokeriya, 2023).

Although these principles help preserve political stability in a diverse region, they also constrain binding forms of cyber cooperation. Consequently, the littoral states face a strategic dilemma: unilateral cyber resilience is insufficient against transnational adversaries that deliberately exploit jurisdictional seams among Indonesia, Malaysia, and Singapore, yet collective action remains politically constrained by entrenched sovereignty sensitivities (Permal & Moorthy, 2024).

This tension points to the need for a shift towards functional cooperation, understood here as operational collaboration that does not depend on full legal harmonisation but instead relies on trusted intermediaries such as ReCAAP ISC,

anonymised data exchange through STIX/TAXII standards, and confidence-building measures such as ADMM-Plus tabletop exercises (Bühler et al., 2023; Ramsdale et al., 2020). Such an approach remains compatible with ASEAN norms while promoting practical resilience, and it offers a realistic pathway for Global South settings where institutional capacity varies but shared vulnerability demands collective action. Without such innovation, the Malacca Strait will remain a bottleneck not only for global trade but also for regional security adaptation. These institutional silos extend beyond national boundaries and become even more pronounced within regional cooperative arrangements.

Cyber Threat Intelligence Practices: Formal Rigidity vs. Informal Fragility

The operational dimension of the governance framework becomes visible through everyday intelligence-sharing practices, in which actors navigate between formal institutional procedures and informal crisis-driven communication channels.

Thematic analysis of 18 semi-structured interviews and 47 policy documents published between 2020 and 2025 indicates the existence of a dual-channel ecosystem for cyber intelligence exchange across the Malacca Strait. Formal channels, such as the ReCAAP Information Sharing Centre (ISC), the ASEAN-Singapore Cybersecurity Centre of Excellence, and Malacca Straits Patrols (MSP) coordination meetings, provide institutional legitimacy and auditability, yet remain poorly configured for cyber threats. As one Malaysian respondent noted, MSP meetings “rarely discuss cyber threats unless they directly affect patrol operations” (MY-04). Likewise, ReCAAP ISC reporting templates do not include fields for cyber indicators such as malware hashes, IP addresses, or attack vectors. Analysts are therefore compelled to fit cyber data into categories originally developed for physical threats such as piracy, reducing analytical precision and weakening response effectiveness. This finding is consistent with earlier studies (Magunna, 2024; Setiawan & Padilla, 2025).

By contrast, informal channels, including military-to-military hotlines, port authority liaison networks, and private-sector information sharing and analysis centres (ISACs), offer speed and flexibility during crises. A Singaporean port cybersecurity lead described using WhatsApp to transmit malware signatures to counterparts in Tanjung Priok, explaining that “It functions effectively during crisis situations, but there’s no record-keeping, and Badan Siber dan Sandi Negara (National Cyber and Crypto Agency, BSSN) never sees these alerts” (SG-05). These ad hoc arrangements enable sub-hour communication, but they lack durability, standardisation, and institutional memory (Senarak, 2025). More importantly, they often exclude civilian cyber agencies such as Indonesia’s BSSN and Malaysia’s National Cyber Security Agency (NACSA), thereby reinforcing civil-military divides during hybrid incidents that require integrated responses (Pramono, 2025).

As shown in Table 3, cyber intelligence-sharing in the Malacca Strait operates through two governance pathways, revealing a persistent tension between speed and accountability that directly affects maritime infrastructure reliability under Sustainable Development Goal (SDG) Target 9.1.

Table 3. Cyber Intelligence-Sharing Channels: Operational Characteristics and SDG
Source: Processed by the Author (2025)

Channel Type	Examples	Strengths	Limitations	SDG Target 9.1 Implications
Formal	ReCAAP Information Sharing Centre (ISC), Malacca Straits Patrols (MSP)	Legally sanctioned, auditable	Slow, often involving delays of 48–72 hours, and not designed for cyber threat indicators	Undermines infrastructure reliability by delaying coordinated response
Informal	Military hotlines, port-level information sharing and analysis centres (ISACs)	Rapid, often under one hour, and flexible during crises	No audit trail, weak institutional memory, and frequent exclusion of civilian agencies	Creates resilience gaps for non-military and cross-sector infrastructure

The coexistence of formal rigidity and informal flexibility creates a persistent trade-off between accountability and responsiveness, ultimately weakening sustained regional resilience. The findings challenge the assumption that institutional proliferation automatically enhances resilience. Instead, overlapping forums generate procedural density without operational coherence, reinforcing what earlier governance research has described as “fragmentation without functional redundancy” (Edwards, 2022).

The role of the private sector is especially significant. Port operators reportedly detect approximately 83% of initial cyber anomalies, including AIS spoofing, ransomware precursors, and network intrusions, yet no secure and legally protected pathways exist for reporting these findings to national authorities (Klar et al., 2023). As one port manager observed, “reporting threats risks exposing our security gaps to competitors” (SG-03). This operational reality reveals a systemic gap: high-fidelity threat intelligence exists, but it remains outside formal response loops because of commercial confidentiality concerns and the absence of liability safeguards.

This dichotomy between formal and informal intelligence-sharing channels points to a deeper structural weakness in regional maritime governance: formal processes remain institutionally inert, whereas informal arrangements are operationally unsustainable. ReCAAP ISC, for example, illustrates institutional path dependency. Its reporting templates, originally developed in the early 2000s to address piracy, remain ill-suited to cyber threats despite the rise of hybrid threat environments (Alaeifar et al., 2024; Saeed et al., 2023; Wang, 2025). This legacy architecture lacks fields for technical indicators such as malware hashes, IP addresses, and attack pathways, making it increasingly inadequate for contemporary cyber-maritime scenarios.

At the same time, reliance on commercial platforms such as WhatsApp, although expedient during emergencies, raises concerns regarding data integrity, confidentiality,

and chain-of-custody requirements relevant to forensic attribution and legal admissibility (Abraham et al., 2025). These informal networks also tend to exclude civilian cyber authorities, including Indonesia's BSSN and Malaysia's NACSA, thereby deepening a problematic civil-military divide (Aji, 2025). During hybrid incidents spanning both physical and digital domains, such as ransomware attacks on port logistics systems, the inability of military hotlines to interface effectively with civilian cyber agencies delays coordinated responses and heightens systemic vulnerability.

This divergence reduces the inclusiveness of regional cyber governance and weakens cross-sectoral resilience. Port operators, who identify a substantial share of early cyber anomalies (Klar et al., 2023), remain excluded from formal intelligence loops because of business confidentiality concerns and the lack of "good faith" liability protections (Rodrigues, 2020). The current system therefore rewards silence rather than disclosure, producing strategic blind spots that adversaries can readily exploit through low-cost, high-impact operations.

These findings call into question a common assumption in security governance, namely that institutional proliferation necessarily leads to greater resilience (Caballero-Anthony, 2020). In the Malacca Strait, the presence of MSP, the Expanded ASEAN Maritime Forum (EAMF), ReCAAP ISC, and the ASEAN-Singapore Cybersecurity Centre of Excellence has produced procedural overlap without operational coherence, a condition that Edwards (2022) characterises as "fragmentation without functional redundancy". Rather than creating additional forums, what is needed is strategic coherence: a minimal, high-trust governance arrangement capable of linking existing nodes through established protocols such as STIX/TAXII, anonymised data exchange, and legal safeguards for good-faith reporting (Christensen, 2023).

Such an approach would help transform the current dual-channel dysfunction into a more coherent and resilient intelligence ecosystem. By decoupling threat sharing from capacity disclosure and incorporating private-sector detection into public-sector response mechanisms, the littoral states could align operational practice more closely with the Sustainable Development Goal (SDG) imperatives of inclusive, multi-stakeholder cooperation and reliable infrastructure. Without such a shift, the region is likely to remain trapped in a cycle of reactive fragmentation, limiting its ability to respond effectively to the adaptive tactics of twenty-first-century hybrid adversaries. These operational tensions reveal governance barriers that cannot be explained by institutional structure alone.

Governance Barriers: The Tripartite Constraint Structure

Integrating the institutional and operational findings discussed above, this subsection identifies a tripartite constraint structure, legal, technical, and political, that helps explain the persistent failure of cross-border cyber threat intelligence (CTI) exchange in the Malacca Strait (Liebetrau & Bueger, 2024).

Thematic analysis of interview transcripts and policy documents reveals three interlocking governance barriers that impede cross-border CTI exchange. Legally, national data sovereignty laws create substantial delays. Undang-Undang Perlindungan

Data Pribadi (Personal Data Protection Law), No. 27/2022 in Indonesia restricts the transfer of “critical infrastructure” data across borders without ministerial approval, causing routine CTI exchange to be delayed by 48 to 72 hours during active incidents (ID-07). Similarly, Malaysia’s Cybersecurity Act 2024 restricts flows of port operational data, while classification mismatches, for example when a cyber intrusion is treated as “Confidential” in Jakarta but “Top Secret” in Singapore, generate procedural deadlock during joint assessments (Cheryl & Ng, 2022; Y. Jin et al., 2025).

Technically, interoperability gaps hinder automated threat correlation (Zibak et al., 2022). Singapore has adopted global standards such as Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) for machine-readable intelligence exchange (Dimitriadis et al., 2021). By contrast, Indonesia and Malaysia continue to rely heavily on unstructured formats such as PDF reports, CSV logs, and email attachments (Ramsdale et al., 2020; Rantos et al., 2020). As one Singaporean analyst noted, “We receive Malaysian indicators of compromise as PDF attachments, we must manually re-key data before correlation, losing 6–8 hours” (SG-05).

Table 4. Governance Barriers to Cross-Border Cyber Threat Intelligence
Source: Processed by the Author (2025)

Barrier Type	Manifestation	SDG Implications	Illustrative Evidence
Legal	Data localisation rules, cross-border transfer restrictions, and classification mismatches	Undermines SDG Target 9.1 by delaying coordinated protection of critical infrastructure	“Indonesian law prohibits sharing critical infrastructure data without ministerial approval” (ID-07)
Technical	Uneven adoption of STIX/TAXII, incompatible data formats, and manual re-keying	Weakens SDG Target 9.b by constraining technology transfer and interoperable digital capacity	“Malaysia uses CSV logs; Singapore uses STIX. Correlation cannot be automated” (SG-05)
Political	Sovereignty-first thinking, strategic mistrust, and reluctance to disclose defensive practices	Undermines SDG Target 17.16 by weakening knowledge-sharing partnerships	“Sharing too much might reveal our defensive weaknesses to neighbours” (MY-06)

Politically, a sovereignty-first mindset continues to shape regional discourse. Interviewees consistently expressed concern that sharing detection methodologies might expose defensive weaknesses. As one Malaysian naval officer stated, “Sharing too much might reveal our defensive weaknesses to neighbours” (MY-06). This perception is reinforced by wider strategic competition in the Indo-Pacific, where cyber capabilities

are often treated as sensitive national assets rather than shared security resources (Subramaniam & Fernandez, 2025).

Barriers to cross-border CTI governance arise through the interaction of legal restrictions, technical incompatibilities, and sovereignty-driven political concerns, revealing the multidimensional nature of cyber-maritime governance constraints.

Table 4 shows that these barriers do not operate independently. Rather, they interact to form a self-reinforcing governance cycle that locks regional cooperation into procedural inertia. This recursive pattern aligns with broader debates on cyber sovereignty in emerging regional orders, where cooperation must coexist with deeply embedded non-interference norms (Hofmann & Pawlak, 2023).

These legal, technical, and political barriers therefore constitute a mutually reinforcing constraint structure. Political mistrust provides the basis for legal rigidity, as states invoke sovereignty to restrict data flows on national security grounds. In turn, these legal constraints legitimise technical minimalism by reducing incentives to invest in interoperable systems such as STIX and TAXII. This cyclical pattern helps explain why growing awareness of hybrid threats has not translated into meaningful collective action.

Legally, data governance regimes in Southeast Asia increasingly treat cyber data as a strategic sovereign asset rather than a shared resilience resource, a pattern that in some respects parallels wider regional debates on cyber sovereignty (Yu & Wang, 2025). This tendency is reflected in Indonesia's Personal Data Protection Law (2022) and Malaysia's Cybersecurity Act (2024), both of which impose restrictions on routine cross-border data transfers without high-level approval. Under this legal logic, CTI is treated not as an operational necessity for resilience, but as a potential national security liability.

Technically, uneven STIX/TAXII adoption reflects wider disparities in institutional capacity. Singapore's more advanced cyber ecosystem, supported by stronger funding, specialised personnel, and integrated civil-military coordination, contrasts with the more resource-constrained settings in Indonesia and Malaysia, where legacy information systems, limited technical expertise, and budgetary constraints hinder standardisation (Klar et al., 2023). Without regional capacity-building efforts, this digital gap is likely to persist and continue to obstruct automated threat correlation.

Politically, ASEAN's principle of non-interference, while important for regional cohesion, can also reinforce zero-sum thinking in the security domain. CTI is often perceived as a form of unilateral exposure rather than mutual reinforcement, particularly in the context of intensifying strategic competition between the United States and China in the Indo-Pacific (Singh et al., 2025). This mindset is compounded by the absence of confidence-building mechanisms, such as joint cyber exercises or transparency protocols, that might gradually transform scepticism into strategic trust among the littoral states.

The interaction between legal rigidity, technical asymmetry, and political mistrust thus produces a self-reinforcing cycle of institutional inertia. The evidence points not simply to a capacity deficit, but to a governance lock-in effect: political mistrust justifies legal restrictions, legal restrictions reduce technical interoperability, and technical incompatibility in turn reinforces mistrust (Hofmann & Pawlak, 2023). This recursive

structure helps explain why escalating hybrid threats have not produced adaptive institutional reform.

Crucially, this tripartite constraint structure directly undermines multiple Sustainable Development Goals, particularly SDG Target 9.1 on reliable infrastructure, SDG Target 9.b on technological upgrading and innovation, and SDG Target 17.16 on knowledge-sharing partnerships. Breaking this cycle requires more than technical improvement; it requires a reconceptualisation of cyber sovereignty itself. As Lawale and Ahmad (2025) suggest, sovereignty in the digital era may be understood as relational capacity, that is, the ability to exercise agency through trusted networks, anonymised data pools, and functional cooperation. Such an approach would decouple CTI exchange from capability disclosure, allowing littoral states to strengthen collective resilience without sacrificing strategic autonomy. Without such a shift, the Malacca Strait is likely to remain exposed to low-cost, high-impact hybrid operations that exploit institutional inertia.

The preceding empirical findings show that governance fragmentation is not merely structural but procedural, embedded in legal rigidity, technical incompatibility, and political mistrust. The proposed Malacca Cyber Intelligence Node (MCIN) blueprint therefore emerges inductively from these observed bottlenecks. Each design feature, including federated architecture, anonymised signal exchange, and model liability safeguards, corresponds directly to one dimension of the tripartite constraint structure identified in this study. Addressing this recursive constraint structure requires governance innovation capable of preserving sovereignty while enabling functional cooperation.

Towards Cooperative Sovereignty: A Critical Analysis of the MCIN Blueprint

Responding directly to the tripartite constraints identified above, this study proposes the Malacca Cyber Intelligence Node (MCIN) as a sovereignty-compatible governance mechanism for operationalising Cooperative Sovereignty. Hosted through the ReCAAP Information Sharing Centre (ISC), MCIN is designed to function within ASEAN's sovereignty-sensitive norms while enabling practical cooperation through technical and legal innovation, thereby addressing key gaps in existing arrangements (Magunna, 2024).

The proposed platform rests on three core elements. First, it employs automated anonymisation processes to remove attribution metadata, such as IP addresses, malware hashes, and sensor locations, from threat indicators before redistribution. This would allow the littoral states to share patterns of hostile activity without disclosing sensitive operational sources or defensive capabilities, thereby reducing sovereignty-related concerns (Lawale & Ahmad, 2025). Second, MCIN adopts an SDG-aligned incident taxonomy informed by International Maritime Organization (IMO) guidance and introduces a mandatory 24-hour notification protocol for incidents affecting port operations, navigational safety, or critical maritime infrastructure, thereby reinforcing the reliability imperative embedded in SDG Target 9.1 (Unctad, 2020; United Nations, 2026). Third, MCIN would be supported by an ASEAN-developed Model Agreement on

Maritime Cyber Data Exchange that provides “good faith” liability protections for participating agencies and private-sector firms disclosing cyber threats under defined conditions (Ferreira & Cavelti, 2025; Hanisch et al., 2025). This legal mechanism is intended to encourage private-sector participation by reducing exposure to commercial and legal risks, thereby addressing the public-private divide identified in the empirical findings.

At the same time, the MCIN proposal raises important structural and political concerns that require careful consideration. First, asymmetries of trust may limit participation. ReCAAP ISC’s institutional proximity to Singapore, a technologically advanced yet geopolitically sensitive actor, may discourage Indonesia and Malaysia from sharing high-fidelity threat data because of concerns that defensive capabilities or operational weaknesses could be inferred indirectly (Lawale & Ahmad, 2025). This perception is likely to be reinforced by longer-standing sensitivities regarding external influence in maritime security governance.

Second, anonymisation may reduce the strategic value of intelligence. Without attribution metadata, recipient states may struggle to assess adversary intent, capability development, or campaign continuity across incidents, thereby limiting MCIN’s utility for strategic warning, threat forecasting, and long-term defence planning (Abraham et al., 2025). Although anonymised data may support tactical response, it is less effective in generating the deeper situational awareness required to address sophisticated or state-linked threat actors.

Third, private-sector participation remains uncertain in the absence of a legally binding Model Agreement on Maritime Cyber Data Exchange adopted by all littoral states. A purely voluntary arrangement may reproduce existing governance gaps, particularly where commercial confidentiality and liability concerns outweigh collective security incentives. This concern is especially relevant to port operators and logistics firms, which detect a large proportion of cyber anomalies but may remain reluctant to report them without credible legal protections (Ferreira & Cavelti, 2025; Hanisch et al., 2025).

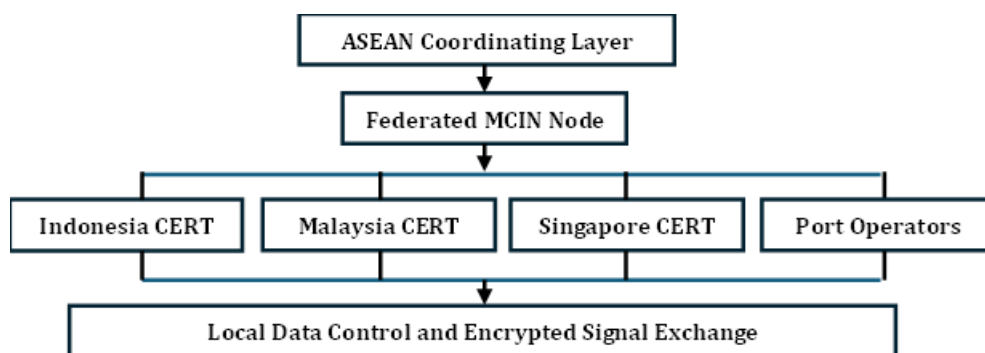


Figure 2. Federated MCIN Architecture

Source: Author’s design based on Fenton (2024) and Peng et al. (2025)

To translate technical exchange into strategic trust, MCIN would need to be complemented by confidence-building measures such as cooperative cyber tabletop

exercises under the ASEAN Defence Ministers' Meeting-Plus (ADMM-Plus) framework. Unlike the European Union's top-down model under the NIS2 Directive (European Commission, 2025), MCIN's sovereignty-preserving design is intended to remain compatible with ASEAN's non-interference principle while still enabling practical resilience.

As illustrated in Figure 2, the proposed architecture consists of an ASEAN coordinating layer linked to a federated MCIN node, which in turn connects national Computer Emergency Response Teams (CERTs) in Indonesia, Malaysia, and Singapore, alongside port operators. This structure preserves local data control while enabling encrypted signal exchange across participating nodes. In this sense, MCIN operationalises the Cooperative Sovereignty framework by combining legal safeguards, anonymised technical exchange, and political confidence-building measures within a federated intelligence arrangement. Rather than replacing existing institutions, it is conceived as an interoperability layer connecting fragmented governance nodes. Its value lies not in transcending sovereignty, but in recalibrating sovereignty as a basis for structured cooperation under conditions of persistent political sensitivity.

Global South Governance Constraints and Scalability

Extending beyond the Malacca Strait case, the findings highlight broader governance constraints characteristic of maritime corridors in the Global South. The design of the Malacca Cyber Intelligence Node (MCIN) emerged inductively from recurring themes identified through thematic analysis. Concerns regarding data sovereignty, classification mismatches, and delayed inter-agency notification directly informed the federated and anonymised architecture proposed in this study.

This suggests that MCIN may offer a scalable model for other Global South chokepoints, including the Strait of Hormuz and Bab el-Mandeb. Theoretically, the model extends Regional Security Complex Theory (Buzan & Wæver, 2003) by demonstrating how functional cooperation may emerge through Cooperative Sovereignty, understood here as a relational practice in which states exercise agency through trusted, anonymised collaboration rather than through isolation. Its viability, however, depends on balancing technical feasibility with political acceptability, a tension that is likely to shape the future of maritime cyber resilience in the Indo-Pacific.

The governance challenges observed in the Malacca Strait are not unique (Caballero-Anthony, 2020). Rather, they reflect broader structural constraints commonly faced by maritime regions in the Global South. These include asymmetries in institutional capacity among littoral states, uneven investment in cybersecurity, dependence on external technology providers, and deeply embedded sovereignty norms that limit supranational delegation of authority. In contrast to higher-capacity Western maritime governance systems, where institutional harmonisation and resource pooling may be more feasible, Global South corridors must navigate a more complex balance between vulnerability exposure, institutional fragmentation, and resource scarcity (Adewumi, 2021; McCabe, 2023).

Recent governance scholarship suggests that cybersecurity resilience in the Global South is shaped less by technological absence than by coordination deficits and normative sensitivities (Fenton, 2024; Peng et al., 2025). This literature shows that fragmentation across agencies, legal classification barriers, and sovereignty-centred diplomatic traditions often impede the development of real-time intelligence-sharing mechanisms (Radanliev, 2025). Accordingly, scalable governance models for maritime cyber resilience must prioritise institutional feasibility and the preservation of sovereignty, rather than rely on centralised enforcement or binding legal harmonisation that may prove politically untenable in such contexts.

Against this backdrop, the proposed MCIN seeks to address these structural challenges by embedding federated coordination within existing institutional arrangements. Rather than introducing supranational authority, the model operates through modular interoperability and anonymised data exchange, thereby aligning with sovereignty-sensitive governance norms (Otto & Jarke, 2019). In this respect, MCIN offers an adaptive governance approach that may be transferable to other Global South maritime corridors characterised by uneven institutional capacity yet shared systemic vulnerability, while also contributing to broader debates on cooperative governance under sovereignty constraints (Chai & Wu, 2025). At the same time, its operational viability remains context-dependent and would require adaptation to local geopolitical and institutional conditions. Collectively, the empirical analysis indicates that maritime cyber resilience depends less on technological capacity alone than on governance arrangements capable of reconciling sovereignty preservation with cooperative intelligence exchange.

Conclusion

This study shows that strengthening maritime cyber resilience in Global South settings requires sovereignty to be re-situated not merely as a constraint, but as a basis for functional cooperation. The findings demonstrate that the principal obstacle to cross-border cyber threat intelligence (CTI) exchange in the Malacca Strait is not infrastructural unreliability alone, but persistent institutional fragmentation, expressed through bureaucratic resistance to cross-border and public-private cooperation. More importantly, this fragmentation is sustained by a tripartite constraint structure in which legal rigidity, technical incompatibility, and political mistrust interact dynamically to reproduce cycles of non-cooperation.

In response, this study advances the Cooperative Sovereignty framework as an alternative analytical lens. By rethinking regional security dynamics beyond the individual state, it shows how states may exercise sovereignty jointly through structured cooperation rather than unilateral control. This challenges the zero-sum assumption that CTI exchange necessarily weakens national security. Instead, the proposed MCIN architecture illustrates how anonymised and federated intelligence-sharing arrangements may strengthen strategic autonomy while enabling collective resilience. In this respect, the framework offers analytical value for Global South scholarship seeking

governance solutions compatible with non-interference norms and limited functional resilience under conditions of growing hybrid threat exposure.

Practically, the MCIN blueprint offers littoral states a possible framework for transforming the Malacca Strait from a zone of vulnerability into a corridor of resilience. By drawing on ReCAAP ISC as a trusted intermediary, introducing incident taxonomies aligned with SDG priorities, and supporting sovereignty-preserving legal arrangements, MCIN provides a structured institutional mechanism for operationalising partnership-based cyber resilience within ASEAN's regional cooperation setting.

Several avenues for future research emerge from this study. First, comparative research could assess the scalability of MCIN in other maritime chokepoints, such as the Strait of Hormuz and the Sulu-Sulawesi Seas, under different geopolitical conditions. Second, quantitative analysis could examine how delays in intelligence-sharing affect infrastructure reliability and resilience outcomes. Third, tabletop exercises simulating MCIN functions during hybrid crises could help test technological arrangements while building confidence among practitioners. Ultimately, the prospects for reducing systemic vulnerability in the Malacca Strait will depend on whether sovereignty-sensitive cooperation can gradually be translated into organised and durable resilience mechanisms.

Acknowledgements

The author gratefully acknowledges the institutional support of Universitas Pertahanan Republik Indonesia in facilitating this research and appreciates the constructive support and collaboration of all stakeholders involved throughout the research process.

References

- Aaronson, S. A., & Leblond, P. (2018). Another Digital Divide: The Rise of Data Realms and its Implications for the WTO. *Journal of International Economic Law*, 21(2), 245–272. <https://doi.org/10.1093/jiel/jgy019>
- Abdullah, M., Nawaz, M. M., Saleem, B., Zahra, M., Ashfaq, E. B., & Muhammad, Z. (2025). Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data. *Analytics*, 4(3), 25. <https://doi.org/10.3390/analytics4030025>
- Abraham, C., Bélanger, F., & Daultrey, S. (2025). Promoting research on cyber threat intelligence sharing in ecosystems. *Journal of Cybersecurity*, 11(1), 1–11. <https://doi.org/10.1093/cybsec/tyaf016>
- Adewumi, I. J. (2021). Exploring the Nexus and Utilities Between Regional and Global Ocean Governance Architecture. *Frontiers in Marine Science*, 8(645557), 1–22. <https://doi.org/10.3389/fmars.2021.645557>
- Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. *Ocean & Coastal Management*, 236, Article 106493. <https://doi.org/10.1016/j.ocecoaman.2023.106493>.

- Agastia, I. G. B. D. (2021). Maritime security cooperation within the ASEAN institutional framework: a gradual shift towards practical cooperation. *JAS (Journal of ASEAN Studies)*, 9(1), 25–48. <https://doi.org/10.21512/jas.v9i1.6919>
- Aji, M. P. (2025). Cybersecurity Politics in Building Cyber Sovereignty in Indonesia Through Strengthening the Role of the National Cyber and Crypto Agency. *Society*, 13(2), 1056–1071. <https://doi.org/10.33019/society.v13i2.960>
- Alaeifar, P., Pal, S., Jadidi, Z., Hussain, M., & Foo, E. (2024). Current approaches and future directions for Cyber Threat Intelligence sharing: A survey. *Journal of Information Security and Applications*, 83(103786), 1–30. <https://doi.org/10.1016/j.jisa.2024.103786>
- Androjna, A., Perkovič, M., Pavic, I., & Mišković, J. (2021). Ais data vulnerability indicated by a spoofing case-study. *Applied Sciences (Switzerland)*, 11(11), 1–25. <https://doi.org/10.3390/AP11115015>
- Bettani, S. A., & Ahmed, Z. S. (2023). China and Regional Security in South and Southeast Asia: A Comparative Analysis of ASEAN and SAARC. *Journal of ASEAN Studies*, 11(2), 289–310. <https://doi.org/10.21512/jas.v11i2.9600>
- Bolbot, V., Kulkarni, K., Brunou, P., Banda, O. V., & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*, 39(100571), 1–18. <https://doi.org/10.1016/j.ijcip.2022.100571>
- Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, 11(4), 589–597. <https://doi.org/10.1080/2159676X.2019.1628806>
- Bühler, M. M., Nübel, K., Jelinek, T., Riechert, D., Bauer, T., Schmid, T., & Schneider, M. (2023). Data Cooperatives as a Catalyst for Collaboration, Data Sharing and the Digital Transformation of the Construction Sector. *Buildings*, 13(2), 1–22. <https://doi.org/10.3390/buildings13020442>
- Buzan, Barry., & Wæver, O. (2003). *Regions and powers : a guide to the global security order*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511491252>
- Caballero-Anthony, M. (2020). Security Governance and ASEAN's Political Security Community: Fragmented but Inclusive Security Communities? *Fudan Journal of the Humanities and Social Sciences*, 13(1), 151–167. <https://doi.org/10.1007/S40647-019-00269-Z/METRICS>
- Chai, Y., & Wu, Y. (2025). The marine community of shared destiny driving paradigm shift in vessel pollution governance: an integrated governance framework for sustainable ocean development. *Frontiers in Marine Science*, 12(1682990), 1–7. <https://doi.org/10.3389/fmars.2025.1682990>
- Chen, J., Lu, Y., Zhang, Y., Huang, F., & Qin, J. (2023). A management knowledge graph approach for critical infrastructure protection: Ontology design, information extraction and relation prediction. *International Journal of Critical Infrastructure Protection*, 43(100634), 100634. <https://doi.org/10.1016/j.ijcip.2023.100634>
- Chen, X., & Gao, X. (2024). Norm diffusion in cyber governance: China as an emerging norm entrepreneur? *International Affairs*, 100(6), 2419–2440. <https://doi.org/10.1093/ia/iaae237>

- Chen, X., & Yang, Y. (2022). Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance. *The International Spectator*, 57(3), 48–65. <https://doi.org/10.1080/03932729.2022.2066841>
- Cheryl, B.-K., & Ng, B.-K. (2022). Protecting the Unprotected Consumer Data in Internet of Things: Current Scenario of Data Governance in Malaysia. *Sustainability*, 14(9893), 1–25. <https://doi.org/10.3390/su14169893>
- Christensen, J. (2023). Studying expert influence: a methodological agenda. *West European Politics*, 46(3), 600–613. <https://doi.org/10.1080/01402382.2022.2086387>
- Cui, D. (2025). Data Sovereignty Disputes and International Cooperation in the Digital Economy of Southeast Asia. In A. Senadjki (Ed.), *Proceedings of the 2025 7th International Conference on Economic Management and Cultural Industry (ICEMCI 2025)* (pp. 933–941). Atlantis Press. https://doi.org/10.2991/978-94-6463-888-2_91
- Dang, V. H., & Mon, S. W. (2023). Improving Maritime Cybersecurity in Southeast Asia: Suggestions for Further Action by asean. *Asia-Pacific Journal of Ocean Law and Policy*, 8, 329–351. <https://doi.org/10.1163/24519391-08020008>
- de la Peña Zarzuelo, I. (2021). Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. *Transport Policy*, 100, 1–4. <https://doi.org/10.1016/j.tranpol.2020.10.001>
- Denzin, N. K. (1978). *The logic of naturalistic inquiry*. McGraw-Hill.
- Dhakal, K. (2022). NVivo. *Journal of the Medical Library Association*, 110(2), 270–272. <https://doi.org/10.5195/jmla.2022.1271>
- Dimitriadis, A., Prassas, C., Flores, J. L., Kulvatunyou, B., Ivezic, N., Gritzalis, D. A., & Mavridis, I. K. (2021). Contextualized filtering for shared cyber threat information. *Sensors*, 21(14), Article 4890. <https://doi.org/10.3390/s21144890>
- Edwards, S. (2022). Fragmentation, Complexity and Cooperation: Understanding Southeast Asia's Maritime Security Governance. *Contemporary Southeast Asia*, 44(1), 87–121. <https://doi.org/10.1355/CS44-1D>
- Emerson, K., Nabatchi, T., & Balogh, S. (2012). An Integrative Framework for Collaborative Governance. *Journal of Public Administration Research and Theory*, 22(1), 1–29. <https://doi.org/10.1093/JOPART/MUR011>
- European Commission. (2025). *The EU Blue economy report 2025: Maritime Affairs and Fisheries (DG-MARE)*. European Commission. <https://op.europa.eu/webpub/mare/eu-blue-economy-report-2025/blue-economic-sectors/maritime-transport.html>
- Fenton, A. J. (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), 2–26. <https://doi.org/10.3390/jmse12030510>
- Ferreira, V. A., & Cavelti, L. (2025). Good Faith and Investment Treaties with a Particular View on Pillar Two. *Intertax*, 53(4), 342–361. <https://doi.org/10.54648/TAXI2025031>

- Flick, U. (2022). *The SAGE Handbook of Qualitative Research Design*. SAGE Publications Ltd
- Fortnam, M., Evans, L., Amira Mas Ayu, A. M., Bastian, L., Chaigneau, T., Creencia, L., Goh, H. C., Gonzales, B., Madarcos, K., Maharja, C., Mohd Iqbal, M., Ngoc Le, T., Praptiwi, R. A., Sugardjito, J., Van Nguyen, Q., & Wan Nur Syazana, W. M. A. (2022). Polycentricity in practice: Marine governance transitions in Southeast Asia. *Environmental Science & Policy*, 137, 87–98. <https://doi.org/10.1016/j.envsci.2022.08.010>
- Hanisch, M., Graf-Vlachy, L., Haeussler, C., König, A., & Cho, T. S. (2025). Kindred spirits: Cognitive frame similarity and good faith provisions in strategic alliance contracts. *Strategic Management Journal*, 46(2), 436–469. <https://doi.org/10.1002/smj.3660>
- Hofmann, S. C., & Pawlak, P. (2023). Governing cyberspace: policy boundary politics across organizations. *Review of International Political Economy*, 30(6), 2122–2149. <https://doi.org/10.1080/09692290.2023.2249002>
- Honrada, G. J. P., & Bokeriya, S. A. (2023). The Shanghai Spirit and the ASEAN Way as the Foundations of a New Regionalism. *Vestnik RUDN. International Relations*, 23(2), 253–264. <https://doi.org/10.22363/2313-0660-2023-23-2-253-264>
- Horst, H. A., Sargent, A., & gaspard, luke. (2024). Beyond extraction: Data strategies from the Global South. *New Media & Society*, 26(3), 1366–1383. <https://doi.org/10.1177/14614448231201651>
- Huang, H., Sun, B., & Hu, L. (2024). A task offloading approach based on risk assessment to mitigate edge DDoS attacks. *Computers & Security*, 140(103789), 1–13. <https://doi.org/10.1016/j.cose.2024.103789>
- Ishkhanyan, A. (2025). The sovereignty-internationalism paradox in AI governance: digital federalism and global algorithmic control. *Discover Artificial Intelligence*, 5(123), 123. <https://doi.org/10.1007/s44163-025-00374-x>
- Jin, X., Huang, S., & Lei, X. (2024). Research on the Impact Mechanism of Green Innovation in Marine Science and Technology Enabling Dual Economic Circulations. *Sustainability (Switzerland)*, 16(19). <https://doi.org/10.3390/SU16198421>
- Jin, Y., Feng, Y., Liu, C., & Li, S. (2025). Navigating the digital seas: Legal challenges and global governance of maritime cyber operations. *Frontiers in Marine Science*, 12, 1616906. <https://doi.org/10.3389/fmars.2025.1616906>
- Khan, A. A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore. *Laws*, 13(4). <https://doi.org/10.3390/laws13040044>
- Klar, R., Fredriksson, A., & Angelakis, V. (2023). Digital Twins for Ports: Derived from Smart City and Supply Chain Twinning Experience. *IEEE Access*, 11, 71777–71799. <https://doi.org/10.1109/access.2023.3295495>
- Lawale, S., & Ahmad, T. (2025). Maritime chokepoints in the Asia-Pacific: geo-economic and security challenges for the GCC states amidst regional and great power competitions. *Asian Journal of Middle Eastern and Islamic Studies*, 19(3), 235–250. <https://doi.org/10.1080/25765949.2025.2595594>
- Liebetrau, T., & Bueger, C. (2024). Advancing coordination in critical maritime infrastructure protection: Lessons from maritime piracy and cybersecurity. *International Journal of Critical Infrastructure Protection*, 46(100683), 1–8. <https://doi.org/10.1016/j.ijcip.2024.100683>

- Louart, M., Szkolnik, J. J., Boudraa, A. O., Le Lann, J. C., & Le Roy, F. (2023). Detection of AIS messages falsifications and spoofing by checking messages compliance with TDMA protocol. *Digital Signal Processing: A Review Journal*, 136. <https://doi.org/10.1016/J.DSP.2023.103983>
- Magunna, A. (2024). Charting waters: the private sector's evolving governance role in Southeast Asian maritime security. *Australian Journal of International Affairs*, 78(3), 306–325. <https://doi.org/10.1080/10357718.2024.2337013>
- McCabe, R. (2023). Environmental drivers of maritime insecurity: governance, enforcement and resilience in the western Indian Ocean. *Conflict, Security & Development*, 23(3), 237–265. <https://doi.org/10.1080/14678802.2023.2256251>
- Melaku, H. M. (2023). A Dynamic and Adaptive Cybersecurity Governance Framework. *Journal of Cybersecurity and Privacy*, 3(3), 327–350. <https://doi.org/10.3390/jcp3030017>
- Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *BMJ*, 339(b2535), 1–8. <https://doi.org/10.1136/bmj.b2535>
- Montfort, S., Fischer, M., Hollway, J., & Jager, N. W. (2023). Design paths of federal intergovernmental cooperation. *Policy Studies Journal*, 51(4), 773–792. <https://doi.org/10.1111/psj.12498>
- Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A Step-by-Step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research. *International Journal of Qualitative Methods*, 22, 1–18. <https://doi.org/10.1177/16094069231205789>
- Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis. *International Journal of Qualitative Methods*, 16, 1–13. <https://doi.org/10.1177/1609406917733847>
- Otto, B., & Jarke, M. (2019). Designing a multi-sided data platform: findings from the International Data Spaces case. *Electronic Markets*, 29(4), 561–580. <https://doi.org/10.1007/s12525-019-00362-x>
- Panke, D., & Stapel, S. (2024). Cooperation between international organizations: Demand, supply, and restraint. *The Review of International Organizations*, 19(2), 269–305. <https://doi.org/10.1007/s11558-023-09506-3>
- Peng, P., Xie, X., Claramunt, C., Lu, F., Gong, F., & Yan, R. (2025). Bibliometric analysis of maritime cybersecurity: Research status, focus, and perspectives. *Transportation Research Part E: Logistics and Transportation Review*, 195(103971). <https://doi.org/10.1016/j.tre.2025.103971>
- Permal, S., & Moorthy, R. (2024). Nuancing Maritime Security Governance in The Straits of Malacca: A Comparative Analysis on Indonesia, Malaysia, and Singapore. *Malaysian Journal of History, Politics & Strategic Studies*, 51(3), 273–292. <https://doi.org/10.17576/jebat.2024.5103.02>
- Pestana, G., & Sofou, S. (2024). Data Governance to Counter Hybrid Threats against Critical Infrastructures. *Smart Cities*, 7(4), 1857–1877. <https://doi.org/10.3390/smartcities7040072>

- Poonnawatt, K. (2023). Multilateral cooperation against maritime piracy in the Straits of Malacca: From the RMSI to ReCAAP. *Marine Policy*, 152(105628), 105628. <https://doi.org/10.1016/j.marpol.2023.105628>
- Pramono, B. (2025). Strategic adaptations for hybrid warfare: Enhancing Indonesian national defence in the digital ERA. *International Journal of Innovative Research and Scientific Studies*, 8(6), 974–981. <https://doi.org/10.53894/ijirss.v8i6.9776>
- Qiao-Franco, G., Karmazin, A., & Kolmaš, M. (2025). The Indo-Pacific and the Next Phase of ASEAN Centrality. *Journal of Current Southeast Asian Affairs*, 44(3), 413–435. <https://doi.org/10.1177/18681034241307658>
- Qu, X., & Meng, Q. (2012). *The economic importance of the Straits of Malacca and Singapore: An extreme-scenario analysis*. Transportation Research Part E: Logistics and Transportation Review, 48(1), 258–265. <https://doi.org/10.1016/j.tre.2011.08.005>
- Radanliev, P. (2025). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, 9(1), 28–78. <https://doi.org/10.1080/23742917.2024.2312671>
- Ramsdale, A., Shiaeles, S., & Kolokotronis, N. (2020). A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages. *Electronics*, 9(824), 1–22. <https://doi.org/10.3390/electronics9050824>
- Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C., & Katos, V. (2020). Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem. *Computers*, 9(18), 1–17. <https://doi.org/10.3390/computers9010018>
- Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, 4. <https://doi.org/10.1016/j.jrt.2020.100005>
- Rosnani, Heryadi, D., M.yani, Y., & Sinaga, O. (2022). Asean maritime security cooperation. *Journal of Maritime Research*, 19(2), 60–64. <https://doi.org/10.12716/1001.16.03.01>
- Rusli, M. H. M., Suherman, A. M., Yuliantiningsih, A., Wismaningsih, & Indriati, N. (2021). *The Straits of Malacca and Singapore: Maritime conduits of global importance*. Research in World Economy, 12(2), 123–131. <https://doi.org/10.5430/rwe.v12n2p123>
- Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors*, 23(16), 1–27. <https://doi.org/10.3390/s23167273>
- Sałek, K., & Fajdek, P. (2025). Analysis of the implementation of the NIS2 directive in the Weimar Triangle countries. *Central European Review of Economics & Finance*, 50(1), 41–52. <https://doi.org/10.24136/ceref.2025.003>
- Senarak, C. (2025). Leveraging advanced technologies and strategies for port cyber resilience: Strengthening incident response and recovery. *Transportation Research Interdisciplinary Perspectives*, 34(101666), 1–25. <https://doi.org/10.1016/j.trip.2025.101666>

- Setiawan, A., & Padilla, A. M. (2025). Addressing Maritime Security Threats in the Malacca Strait: A Malaysian Perspective. *Open Journal of Social Sciences*, 13(02), 333–359. <https://doi.org/10.4236/jss.2025.132021>
- Sharma, L. (2024). Maritime cybersecurity in the Indo-Pacific: envisioning a role for the Quad. *Journal of the Indian Ocean Region*, 20(1), 14–36. <https://doi.org/10.1080/19480881.2024.2341467>
- Singh, N. K., Jash, A., & Nanjappa, Y. (2025). Navigating the nexus: geopolitical, international relations and technical dimensions of US-China cyber strategic competition. *Cogent Social Sciences*, 11(1), 1–18. <https://doi.org/10.1080/23311886.2025.2499171>
- Soner, O. (2025). Modeling and analyzing cybersecurity risk propagation in ports using fuzzy cognitive maps: System sensitivity to key threat factors. *Ocean & Coastal Management*, 270(107857), 1–12. <https://doi.org/10.1016/j.ocecoaman.2025.107857>
- Soner, O., Kayisoglu, G., Bolat, P., & Tam, K. (2024). Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks. *Applied Ocean Research*, 142(103855). <https://doi.org/10.1016/j.apor.2023.103855>
- Subramaniam, G. A. M., & Fernandez, K. (2025). Contested Waters, Contested Futures: The South China Sea Security Complex and Malaysia's Sabah Dilemma. *AEI Insights*, 10(1), 56–69. <https://doi.org/10.22452/AEIINSIGHTS.vol10no1.5>
- Tenny, J. A., & Kassim, A. (2025). Strategic Pathways for Resilience in Maritime Governance in Southeast Asia: A Systematic Literature Review. *Proceedings of the 2nd International Conference on Administrative Science (ICAS 2024)*, 717–732. https://doi.org/10.2991/978-94-6463-791-5_72
- Tikanmäki, I., & Ruoslahti, H. (2024). Exploring crisis management response to hybrid threats and warfare. *Journal of Military Studies*, 1(1), 1–12. <https://doi.org/10.2478/jms-2024-0009>
- Triwahyuni, D., Anggraeni, S., Iqbal, M., Fadilla, N. T., & Mokoginta, F. (2025). *Strengthening Indonesia's Cybersecurity Through Cooperation in The ASEAN Regional Forum* (pp. 131–148). https://doi.org/10.2991/978-2-38476-442-6_13
- Tuan Binh, N., Xuan Hiep, T., & Hoang Long, T. (2022). Maritime Security in the Indo-Pacific Region: A View from the Geostrategic Position of The Malacca Strait. *AUSTRAL: Brazilian Journal of Strategy & International Relations*, 11(21), 115–131. <https://doi.org/10.22456/2238-6912.119787>
- Unctad. (2020). *Trade And Development Report 2020: From Global Pandemic to Prosperity for All: Avoiding Another Lost Decade*. United Nations Publications.
- United Nations. (2026). *Review Of Maritime Transport 2025: staying the course in turbulent waters*. United Nations Publications.
- Wang, Q. (2025). Managing emerging port security challenges in developing green and digital shipping corridors: A port governance cooperation perspective under the Belt and Road Initiative. *Ocean & Coastal Management*, 270(107924). <https://doi.org/10.1016/j.ocecoaman.2025.107924>
- Weaver, G. A., Feddersen, B., Marla, L., Wei, D., Rose, A., & Van Moer, M. (2022). Estimating economic losses from cyber-attacks on shipping ports: An optimization-based

- approach. *Transportation Research Part C: Emerging Technologies*, 137. <https://doi.org/10.1016/j.trc.2021.103423>
- Xu, W., & Zuo, X. (2026). Confronting Cross-Border Data Risks. *Journal of Global Information Management*, 34(1), 1–25. <https://doi.org/10.4018/JGIM.399056>
- Yu, M., & Wang, L. (2025). China's cross-border maritime data flow governance: Progress, challenges, and prospects. *Frontiers in Marine Science*, 12, 1600050. <https://doi.org/10.3389/fmars.2025.1600050>
- Zibak, A., Sauerwein, C., & Simpson, A. C. (2022). Threat intelligence quality dimensions for research and practice. *Digital Threats: Research and Practice*, 3(4), 1–22. <https://doi.org/10.1145/3484202>