Maritime Critical Infrastructure in Southeast Asia: Policy Frameworks and Resilience

Deniz Kocak

Structured Abstract

Article Type: Research Article

Purpose—This study examines how Southeast Asian states can ensure their critical maritime infrastructure's security in the face of hybrid threats and geopolitical tensions through technological innovation and regional cooperation.

Design, Methodology, Approach—Applying Balzacq's practice-centered securitization framework and Krippendorff's content analysis, the study examines defense documents from five Southeast Asian states and the Association of Southeast Asian Nations (ASEAN) Maritime Outlook across four dimensions: threat concepts, technological approaches, governance structures and regional cooperation mechanisms.

Findings—Southeast Asian states share threat perceptions but differ in priorities and tech capacity: Singapore leads with AI and digital twins, while Vietnam relies on conventional deterrence. Cooperative arrangements like the Malacca Straits Patrol remain geographically confined, while sovereignty concerns and differing conceptions of hybrid threats impede integrated regional defense concepts.

Practical Implications—States should adopt modular, threat-specific cooperation rather than broad multilateral schemes and pair tech modernization with institutional reforms that reconcile sovereignty with shared vulnerability management.

Originality, Value—Through Balzacq's securitization theory, this study links technological capacities, governance structures and cooperation mechanisms in Southeast Asian maritime security, demonstrating how hybrid threats are constructed through practice-centered processes rather than speech acts. It expands theory on how hybrid threats redefine the gray zone between war and peace.

Helmut Schmidt University / University of the Federal Armed Forces Hamburg: kocakd@hsu-hh.de.

Journal of Territorial and Maritime Studies / Volume 13, Number 1 / Winter/Spring 2026 / pp. 30–49 / ISSN 2288-6834 (Print) / DOI: 10.2307/JTMS.13.1.30 / © 2026

Keywords: critical maritime infrastructure, hybrid threats,
regional security cooperation, resilience, Southeast Asia

I. Introduction

The sabotage of the Nord Stream pipelines in September 2022 marked a turning point in international perceptions of maritime infrastructure security. This incident in the Baltic Sea exposed the vulnerability of subsea systems and illustrated how such assets can serve as leverage in international conflicts.[1] In Southeast Asia, where maritime infrastructure forms the backbone of both regional and global economies, similar security concerns have developed. The Strait of Malacca is a global trade hub, and the dense networks of undersea cables and the region's exposed energy supply lines are increasingly the focus of hybrid threat scenarios.[2] Maritime infrastructure refers to five key areas: transport infrastructure (e.g., ports and shipping routes), energy infrastructure (offshore platforms and undersea pipelines and cables), fisheries infrastructure, and marine biodiversity systems.[3] Threats in the maritime domain highlight the limits of conventional protection mechanisms. The blurring of military and civilian threats, targeted exploitation of international law loopholes and increasing digitalization of maritime systems demonstrate that existing protection mechanisms for critical maritime infrastructure require reconsideration.[4]

Hybrid threats in the maritime domain refer to coordinated actions below the level of conventional warfare that combine military, political, economic, legal and informational means to exploit vulnerabilities in maritime systems.[5] Resilience describes the systematic ability of all social subsystems to ward off such threats through protection, adaptation and restoration measures, taking into account mutual dependencies, a pattern of responses to internal or external shocks that aims to preserve, slightly modify or fundamentally transform a reference object.[6]

This blurring also exemplifies what Balzacq[7] distinguishes as the challenge of differentiating between "institutional threats" and "brute threats." This theoretical distinction gains particular prominence when assessing how Southeast Asian states reconcile traditional security concerns with emerging hybrid challenges.

New forms of hybrid threats increasingly impact the security landscape. Cyberattacks on ship navigation systems, coordinated disinformation campaigns and targeted manipulation of regulatory processes make it difficult to draw a clear distinction between warlike and peaceful actions.[8] These gray-zone activities require a thorough reassessment of existing security concepts, as they not only make it difficult to clearly attribute incidents to their perpetrators, but also undermine the effectiveness of conventional deterrence strategies. Attacks on undersea cables or disruption of harbor operations can cause economic and social damage without open military confrontation.

Moreover, Southeast Asian security policy dynamics are characterized by strategic competition between major powers. The US–China rivalry is turning Southeast Asia into a theater of geopolitical conflict, where maritime infrastructure gains strategic importance.[9] This development is forcing ASEAN countries to make strategic considerations: while some members, such as the Philippines, are considering closer security ties with the US, others,

such as Indonesia, are seeking to preserve their strategic autonomy in the competition between major powers through a policy of active non-alignment.

Given these overlapping challenges, a central puzzle emerges: Why do different security stakeholders in Southeast Asia pursue divergent technological and governance solutions to hybrid threats against maritime infrastructure, despite facing shared vulnerabilities? This divergence is particularly puzzling given that hybrid threats require coordinated, multilateral responses. If maritime security actors acknowledge the transnational character of these threats, what explains the persistence of fragmented, nationally oriented approaches? Moreover, how can coherent regional governance mechanisms be developed when states operate under different security cultures, technological capabilities, and strategic alignments with extra-regional powers?

Building on this puzzle, this study examines why divergent approaches persist and how Southeast Asian states can develop more coherent strategies to ensure the security of their critical maritime infrastructure through technological innovation and regional cooperation. It encompasses both technological innovation and regional cooperation. The study draws on Balzacq's[10] sociological account of securitization understood as a practice-centered process. Rather than privileging singular speech acts, the approach foregrounds how security problematizations are enacted through instruments and organizational arrangements (dispositifs) within specific contexts. The study therefore examines which referent objects are portrayed as being at risk, the contextual conditions that allow particular problematizations to gain traction, and how the documents articulate the linkage to technologies, procedures and rules.

The academic relevance of this study lies in the systematic analysis of a hitherto insufficiently integrated research field. The existing literature fragments maritime security into discrete analytical silos. An integrative framework linking these dimensions remains absent. This study attempts to close this gap through comprehensive analysis of official security documents from the region. From a policy perspective, the study examines how resilience concepts are designed and presented in Southeast Asian national defense strategies. The region is characterized by technological and institutional imbalances, making common security approaches difficult. The comparative analysis of the Defence White Papers reveals different approaches and potential impediments in strategies. The results can provide guidance for the development of harmonized regional security approaches and can also serve as a basis for decision-makers in shaping future defense concepts. Furthermore, insights into the interactions between technological capabilities, governance structures and regional cooperation mechanisms in response to hybrid threats provide new perspectives for international security research. Using qualitative content analysis after Krippendorff,[11] the paper examines national defense and maritime security documents from Singapore, Malaysia, Indonesia, the Philippines, Vietnam, and the *ASEAN Maritime Outlook* across four dimensions: threat concepts, technological approaches, governance, and regional cooperation. Across the empirical sections, recurrent storylines and their intertextual reproduction are highlighted where documents link problematizations to envisaged instruments or procedures.

Following this introduction, the literature review systematizes the current state of research on maritime critical infrastructure in Southeast Asia. The subsequent methods chapter explains the analytical procedure of the structured content analysis in detail. The

empirical analysis presents the results along the four dimensions of the study, and the synthesis summarizes the findings and develops overall insights into the possibilities and limitations of technological and cooperative security strategies. The conclusion reflects on the theoretical and practical implications for maritime security in Southeast Asia and beyond. In resolving the puzzle of divergent security approaches, the study contributes to both securitization theory and practical policy coordination in the Indo-Pacific maritime domain.

II. Literature Review

The security of maritime critical infrastructure has become a central field of research. Modern societies are ever more dependent on networked systems, while hybrid threats are becoming increasingly complex. Southeast Asia holds a central position in this context. The region is geographically and geopolitically at the center of global maritime networks. This literature review examines the current state of research on how states in Southeast Asia can ensure the security of their critical maritime infrastructure through technological innovation and regional cooperation.

2.1 Conceptualizing Maritime Criticality

Academic and policy-oriented debates on maritime critical infrastructure face definitional challenges. Maritime security remains controversial as a concept because the actors involved pursue divergent priorities; for example, navies focus on strategic and defense considerations, whereas private and trading companies foreground commercial interests.[12]

This divergence raises a fundamental question: if the transnational nature of hybrid maritime threats necessitates coordinated responses, why do such fragmented approaches persist across the region? The conceptual challenge is exacerbated when maritime critical infrastructure is understood as a highly politically dependent concept. Bueger and Liebetrau[13] categorize maritime infrastructure into five main areas: transport, energy, communication, fisheries and marine biodiversity. This categorization shows the different dimensions of the object of investigation.

The Asian Development Bank[14] focuses on functional aspects when defining critical infrastructure in the Asia-Pacific context. Essential infrastructure systems are primarily assessed according to the extent to which their disruption can have a serious impact on the economy, public health and social stability. While the analysis covers system-wide and long-term risks, the technological specifics of individual infrastructures are hardly considered. Cannon[15] fills this gap with his detailed analysis of undersea cables. He identifies them as infrastructures that transport over 95 percent of global internet traffic and enable communication and financial transactions.

Wang et al.[16] classify the Strait of Malacca, together with Gibraltar, as the most strategically important sea choke points globally, emphasizing their central role in maritime transport. The Boston Consulting Group[17] also points out that around 30% of global trade and around two-thirds of Chinese trade, and therefore around 80% of its energy imports, pass through the Strait of Malacca. Moreover, Till[18] places this geographical conditionality in a larger analytical context. Maritime infrastructure in Southeast Asia has two main

functions: it connects global shipping routes and supports the region's energy supply. This overlapping of different functions makes one-dimensional security approaches obsolete. Consequently, integrated protection frameworks must capture and accommodate the full spectrum of challenges inherent in this maritime domain.

2.2 From Traditional to Hybrid Threats

Since the annexation of Crimea by Russia in 2014, hybrid threats have increasingly become the focus of security policy research. Mitrescu and Sokolov[19] point out that the topic of *hybrid threats* has since become an independent discipline within security research. They define hybrid threats, also in the maritime domain, as coordinated activities below the threshold of conventional warfare that specifically combine different military, political, economic, legal and informational means. Fenton[20] uses a case study on the Strait of Malacca and Singapore to illustrate the growing hybrid risks posed by the increasing networking of marine IT and operational IT. The author notes that cyber security standards in the maritime sector lag behind those of other critical infrastructure sectors. Accordingly, this indicates that the likelihood of incidents, such as malware, ransomware or targeted manipulation of navigation systems, is increasing due to outdated systems and growing attacker expertise. Underwater cables vividly demonstrate the vulnerability of critical infrastructure and its practical implications. Submarine cables in the South China Sea region are increasingly becoming the center of hybrid threats in which targeted political influence, regulatory blockades and deliberate creation of dependencies are becoming a "weapon." Over the past decade, the distinction between unintentional failure and deliberate attack has become blurred, which in turn makes reliable attribution challenging. Dual-use technology, proxy infrastructure, and rising system complexity all create plausible alternative causes for incidents.[21] Also, as Scholvin and Wigell[22] predicted back in 2019, energy pipelines and maritime hubs are increasingly becoming the center of international competition. The sabotage of the Nord Stream pipelines in the Baltic Sea in 2022 illustrates the growing strategic importance of critical infrastructure in the context of geo-economic power politics. The concept of resilience has established itself as a central theoretical approach to cope with the identified threats. Gharehgozli et al.[23] develop a four-stage framework that specifically addresses the challenges to which seaports are exposed as a result of natural disasters and socio-political risks. Their approach emphasizes that resilience cannot be reduced to technical protection measures alone, but also encompasses organizational, economic and social dimensions. According to Gharehgozli et al., particularly in the context of Southeast Asia, where maritime infrastructure is simultaneously exposed to natural disasters and geopolitical challenges, it is evident that effective resilience strategies require the continuous analysis of risks, the involvement of various stakeholders and the ongoing adaptation and improvement of measures. The framework thus emphasizes the need to understand resilience holistically and as a dynamic, long-term process that goes far beyond traditional technical approaches.

2.3 Technological Responses and Limitations

The practical implementation of resilience concepts is increasingly being realized through technological innovations in the field of maritime domain awareness. Developments range from traditional surveillance systems such as radar and AIS to the increased use of satellites and

the integration of advanced information and communication technologies, including artificial intelligence. This technological development is continuously improving monitoring capacities and the networking of relevant actors.[24] However, Bueger and Edmunds[25] emphasize that technological surveillance systems and innovative information platforms alone are not enough to effectively address maritime security problems. These technologies will only be effective if appropriate institutional capacities, coordination mechanisms and analytical capabilities are developed. This understanding is particularly relevant for Southeast Asia, where the technological capacities of different states vary considerably. Moreover, technological solutions alone cannot address the challenge of fragmented regulatory authority.

2.4 Governance Gaps and Sovereignty Challenges

The monitoring of underwater infrastructure also provides an example of the limits of purely technological solutions. Kraska[26] analyzes the restrictions under international law that stand in the way of effective monitoring in international waters. The installation of permanent sensor systems outside national jurisdiction remains legally controversial, but this creates significant gaps in the protection concept. Technological challenges exacerbate these legal limitations. Kajiwara[27] addresses the rapid proliferation of military AUV programs in the region. However, their applicability for the protection of civilian infrastructure remains unclear. The dual-use problem of these technologies also complicates regional security cooperation, as military and civilian applications are difficult to separate.

The governance of maritime critical infrastructure is characterized by an ambiguity of responsibilities. Their transnational significance contrasts with fragmented regulatory structures. Girardi and Ebrard[28] identify the unclear allocation of responsibility as a core problem. As most underwater infrastructure is privately owned, this creates a regulatory gray area. On the one hand, state responsibility for safety overlaps with private sector interests. On the other hand, national jurisdictions overlap in maritime areas, which further complicates the situation. This creates a regulatory vacuum. While Tan[29] argues for an increased involvement of private actors through public-private partnerships, the US and India, take a state-centered approach. Their establishment of government-led cable ship programs keeps critical repair and maintenance capabilities under direct government control. These divergent approaches reflect different political economies and security cultures. However, they make it difficult to develop coherent regional governance mechanisms.

2.5 Regional Cooperation: Ambitions Versus Implementation

Analyzing regional cooperation mechanisms reveals a paradoxical picture. The need for coordinated approaches in the face of cross-border threats is evident. However, the existing structures fall short of the requirements. Accordingly, Edwards[30] argues that within the numerous ASEAN arrangements on maritime security, there are discrepancies between ambitious declarations and their actual implementation, reflecting divergences of interest among member states, particularly with regard to maritime risks and their prioritization. Despite structural deficits, successful models of sub-regional cooperation exist. Poonnawatt[31] analyzes the Malacca Straits Patrol as an example of functioning maritime security cooperation. The Malacca Straits Patrol (MSP), which has been active since 2004,

combines maritime and air surveillance with intelligence sharing between Indonesia, Malaysia, Singapore and Thailand. This has led to a decline in piracy incidents in the Strait of Malacca.[32] Similarly, the Trilateral Cooperative Arrangement in the Sulu and Celebes Sea areas enables coordinated sea/air patrols with information exchange against cross-border risks such as kidnappings and piracy.[33] The success of these minilateralism initiatives is based on the fact that they circumvent ASEAN's consensus-oriented decision-making process, which has been slowed down since the 1990s by enlargement and diverging national interests.[34] However, Davenport[35] argues that the MSP model is not easily transferable to the protection of underwater infrastructure. Sovereignty concerns, protection of technological information and different threat perceptions represent structural obstacles.

The security of maritime critical infrastructure in Southeast Asia is also closely linked to the overarching geopolitical dynamics of the region. Govella[36] analyzes how the securitization of the maritime domain through the US–China rivalry influences and constrains the policy space of regional actors. The security discourse varies considerably, not only from country to country but also within individual countries and sectors. This discursive fragmentation makes it difficult to develop common threat analyses and coherent regional protection strategies, as Govella[37] argues. The application of classic deterrence theories to the protection of maritime infrastructure proves to be problematic. As Platte[38] points out, the difficult attribution of attacks, uncertainties in the selection and calibration of appropriate responses and doubts about the credibility of threats of retaliation make effective deterrence particularly difficult. Physical factors exacerbate these challenges in the maritime context. For example, the inaccessibility of many infrastructures and the difficulty of forensic investigations underwater make clear attribution difficult, thus hampering a credible response.

III. Methodology

This study adopts a qualitative research design and draws on a systematic reading of official security documents and policy papers to trace how security concepts and cooperation mechanisms for maritime critical infrastructure are articulated in Southeast Asian states. A qualitative approach was chosen since it captures implicit security logics and discursive threat constructions that are not readily accessible through quantitative techniques.[39]

As for the corpus and case selection, the document sample covers the latest available national defense white papers and maritime security strategies from Singapore, Malaysia, Indonesia, the Philippines, and Vietnam. These cases were purposively selected because they sit astride strategic sea lanes yet embody diverse approaches to maritime security. As Singapore does not publish a defense white paper,[40] functionally equivalent official materials were used. To also capture a regional vantage point, the *ASEAN Maritime Security Outlook* is included. Selection followed simple, transparent criteria: (1) official government publications issued after 2020 to reflect current security conceptualizations; (2) top-level policy documents to ensure authoritative statements of national positions; and (3) availability in English for analytical consistency. The analysis combines a structured, focused reading with a compact codebook (see Table 1). Initial categories, *threats, technology, governance, and cooperation*, were informed by the maritime security literature. These also align with Balzacq's levels of securitization analysis, where threats relate to referent objects,

technology to dispositifs, and cooperation to intersubjective processes.[41] The categories are operationalized as four dimensions for cross-case comparison. Specific guiding questions were then created inductively during preliminary reading. Before full analysis, these questions were fixed to preserve comparability across cases, consistent with Krippendorff's insistence on stability in the measurement procedure.[42]

The first dimension identifies and prioritizes specific threats to maritime critical infrastructure, distinguishing traditional from hybrid threats and specifying the actors attributed to them. It also attends to assessments of infrastructure vulnerability and the anticipated time horizons of threat scenarios. The second dimension evaluates proposed technological solutions, considering the balance between surveillance, resilience and physical protection, the explicit role of emerging technologies (especially artificial intelligence and autonomous systems), and issues of technological dependencies, sovereignty and capacity gaps. The third dimension assesses governance arrangements, particularly the allocation of responsibilities between state authorities and private infrastructure operators. The fourth dimension examines regional cooperation, identifying prioritized bilateral or multilateral formats and conceptions of ASEAN's role, and analyzing proposed information exchange, operational cooperation, and how sovereignty concerns are balanced with cooperative needs.

In line with Krippendorff's distinction between sampling, context and recording units, the respective document is the sampling unit; sections and chapters provide context; and the recording unit is a semantically coherent passage directly addressing maritime critical infrastructure.[43] For each subcode in Table 1, there is a note whether the text offers only a general gesture or a specific claim. A simple 0–2 scale is used for this purpose (0 = not mentioned; 1 = general/vague; 2 = specific-named measure/system/format/institution). Subcodes within a dimension are applied exclusively, and cross-dimension double coding is allowed where substantively warranted, in keeping with Krippendorff's emphasis on explicit decision rules and category separability.[44] The table notes beneath Table 1 summaries these conventions.

The four dimensions were applied systematically to each document. Relevant passages were coded, condensed, and summarized in a comparative matrix. This enables within-case coherence checks and cross-case contrasts. Guiding questions were lightly refined during initial readings for clarity and fit, after which they remained stable. Where a document omits a dimension, this is explicitly recorded as an informative silence rather than treated as missing data. As for the scope and potential limitations, the analysis concerns declared positions in official texts. However, it does not test causal mechanisms or implementation outcomes. The aim of this study was comparability of meaning across a focused set of cases, not statistical generalization.

Table 1: Condensed Codebook for Maritime Critical Infrastructure Analysis.

Dimension	Subcode	Definition	Key decision rule	Scale
Threats	Traditional	Physical/conventional maritime risks (e.g., piracy, armed attacks).	Only here if not framed as gray-zone/hybrid.	0/1/2
Threats	Hybrid/Gray-zone	Mix of non-kinetic means (cyber, information, economic) with/without limited kinetic elements.	Requires two domains or explicit "hybrid/gray-zone" framing.	0/1/2

Dimension	Subcode	Definition	Key decision rule	Scale
Threats	Actors/Attribution	Named state/non-state perpetrators or clear attribution.	Foreign actors = 1; named/type + context = 2.	0/1/2
Threats	Vulnerability/Time horizon	Concrete KMI weak points and temporal outlook.	Named assets/segments or timeframes = 2.	0/1/2
Technology	Surveillance/ISR/MDA	Sensors, C2/C4ISR, maritime domain awareness.	Specific platform/system or network named = 2.	0/1/2
Technology	Resilience/Hardening	Redundancy, backup, recovery time, critical node protection.	Standards/plans/metrics specified = 2.	0/1/2
Technology	Physical protection/Forces	Access control, patrols, infrastructure hardening, security forces.	Concrete forces/plans/assets = 2.	0/1/2
Technology	AI/Autonomous systems	Explicit AI analytics or unmanned/autonomous systems for MDA/protection/response.	Vague "smart tech" ≠ 2; named use-case/system = 2.	0/1/2
Technology	Sovereignty/Dependencies	Domestic capability vs. import/partner reliance.	Source/alternatives/industrial strategy specified = 2.	0/1/2
Technology	Capacity gaps/Plans	Stated capability gaps plus programmes/timelines to address them.	Budget/programme/timeline named = 2.	0/1/2
Governance	Lead agency/Roles	Clear allocation of responsibilities state/operator/authorities.	"Whole-of-government" only = 1; named lead + remit = 2.	0/1/2
Governance	Inter-agency coordination	Formal mechanisms across ministries/agencies.	Bodies/SOPs/joint centres/task forces specified = 2.	0/1/2
Governance	Law/Regulation/Standards	Laws, regulatory frameworks, audits, compliance.	Named law/regulation/standard + scope = 2.	0/1/2
Governance	Crisis management/Response	Contingency plans, exercises, alert/recovery processes.	Named exercise/plan/centre = 2.	0/1/2
Co-operation	Formats/Levels	Bilateral, minilateral, ASEAN frameworks; external partners.	Specific forum/arrangement/initiative named = 2.	0/1/2
Co-operation	Functions/Instruments	Info-sharing, exercises, combined ops, SOP harmonisation, capacity building.	Concrete mechanism/workstream = 2.	0/1/2
Co-operation	Sovereignty vs. Interoperability	Balance of national control with data/ops sharing needs.	Explicit red lines/data-sharing rules/EEZ references = 2.	0/1/2
Co-operation	External partners	Role of non-ASEAN partners in maritime security.	Partner/programme/TTX named = 2.	0/1/2

Recording unit: Semantically coherent passage on MCI security (≈ 1–5 sentences).
Scale (specificity): 0 = not mentioned; 1 = general/vague; 2 = specific (named measure/system/format/institution).
General decision rules: Subcodes within a dimension are mutually exclusive; cross-dimension double coding are allowed.

IV. Analysis of Maritime Security Concepts for Critical Infrastructure in Southeast Asia

This analysis examines the security concepts of selected countries in Southeast Asia regarding maritime critical infrastructure. The focus is on threat perceptions, technological approaches, institutional structures and cooperation forms. The central categories of threat concepts, technological security approaches, governance structures and regional cooperation mechanisms were formed inductively.

4.1 Dimension 1: Threat Concepts for Maritime Critical Infrastructure

This subsection identifies how documents problematize specific maritime threats, the context conditions invoked, and whether these framings are coupled to envisaged instruments, procedures, or rules. Southeast Asian defense documents reveal varying threat perceptions. These reflect Balzacq's "semantic repertoires of security."[45] Malaysia identifies US–China geopolitical rivalry as the primary structural challenge to regional security. Malaysia also identifies both Chinese militarization and American naval operations as transforming the South China Sea into a great power arena.[46] This assessment contrasts with Indonesia's assessment, which distinguishes between factual threats such as terrorism, separatism and piracy and non-factual threats, prioritizing the former.[47] The Philippines position the conflict in the West Philippine Sea as their top security challenge. Massive artificial island construction in Philippine waters by China is explicitly classified as a serious threat to national security.[48] Vietnam adopts a more abstract approach without direct attribution of actors. Instead, unilateral actions, power-based coercion and violations of international law are identified as primary threats.[49] Singapore perceives an increasingly dangerous security environment resulting from growing international tensions and its exposed position as a geostrategic hub in Southeast Asia's transport and trade network.[50]

Hybrid threats are conceptualized with varying definition precision in the documents analyzed. This variation illustrates Balzacq's argument that securitization employs different "heuristic artifacts," for example metaphors, stereotypes, and emotions, contextually mobilized by securitizing actors.[51] Indonesia explicitly defines hybrid threats as combining military and non-military elements.[52] Malaysia describes hybrid conflicts as occurring across multiple domains.[53] The Philippines demonstrates an implicit understanding of hybrid threats by linking territorial disputes with environmental degradation. For instance, the construction of artificial terrain has already inflicted irreversible ecological damage, decimating marine resources in traditional fishing grounds.[54] Vietnam avoids explicit terminology, but describes the combination of information warfare and cyber warfare by enemy forces as a particularly dangerous multidimensional threat.[55]

Indonesia's outermost islands, Malaysia's territorial divide, and Singapore's cable hub status create distinct yet interconnected vulnerabilities. These assessments reveal how states identify different "referent objects," things seen as existentially threatened with legitimate claims to survival, ranging from outermost islands to strategic waterways.[56] Indonesia emphasizes its vulnerability as an open archipelago with 92 outermost islands, 12

requiring priority protection.[57] Malaysia, by contrast, identifies the territorial divide created by the South China Sea as a major operational challenge. Both states nevertheless underscore the need to secure four strategic waterways: the Strait of Malacca, the South China Sea, the Sulu Sea and the Sulawesi Sea.[58] The Philippines emphasizes dependence on sea lanes, which must remain open to ensure freedom of trade and navigation.[59] And Vietnam recognizes its geostrategic position as a bridge linking East Asia and Southeast Asia, spanning vital sea lanes connecting the Pacific and Indian Oceans.[60]

The ASEAN Maritime Outlook presents a regional perspective focusing on transnational threats. Piracy and armed robbery against ships persist, with documented increases in incidents near the Straits of Malacca and Singapore in 2022.[61] Cyberattacks emerge as threats to the maritime sector, disrupting ship operations and maritime trade.[62] Illegal, unreported and unregulated fishing presents a multidimensional threat affecting marine environment and working conditions on fishing vessels.[63] These varied threat conceptualizations directly influence the technological approaches states adopt for maritime security.

4.2 Dimension 2: Technological Security Approaches

The technological security approaches demonstrate significant technological disparities. These technological tools function as what Balzacq[64] calls "dispositifs," material anchors of security problematizations that embody specific threat images.

Singapore presents the most advanced portfolio with the world's first Maritime Digital Twin. This system uses artificial intelligence and predictive analytics for port operations optimization, integrating real-time data for improved decision-making in maritime operations management.[65] The Maritime Cyber Assurance and Operations Centre provides real-time cybersecurity monitoring, disseminates threat information and offers system recovery advice.[66] Vietnam focuses primarily on conventional deterrence capabilities. The country deploys SSK Kilo-class submarines, Gepard 3.9 frigates, Project 12418 missile corvettes and Bastion mobile coastal defense systems.[67] This prioritization of conventional weapon systems reflects Vietnam's focus on territorial defense. In contrast, Malaysia, Indonesia and the Philippines are pursuing the same basic principle: C4I-supported ISTAR for a networked maritime situation awareness. Malaysia is increasing its maritime domain awareness with maritime reconnaissance aircraft and MALE drones.[68] Indonesia is linking satellite and UAV data in a planned C4IOR network to support its Global Maritime Fulcrum strategy,[69] and the Philippines is introducing a C4ISTAR system that connects all branches of the armed forces for synchronized joint operations.[70] These systems function as what Balzacq[71] categorizes as "capacity tools," instruments that enable agencies to make decisions and carry out activities with reasonable probability of success.

Also, the balance among surveillance, resilience and physical protection varies considerably across the countries analyzed. Singapore demonstrates the most integrated approach. The Maritime Digital Twin combines all three elements through risk assessments for incidents such as oil spills while optimizing energy efficiency and emissions reduction.[72] Malaysia pursues an integrated multi-layered air defense approach with concurrent development of Network Centric Operations for improved decision-making.[73] The Philippines emphasize acquiring equipment providing nationwide 24/7 domain awareness.[74] Moreover, Singapore leads in developing of AI-supported technological solutions for

cyber defense. The MPA-TalTech collaboration explores substantial opportunities for cyber defenders through AI-enabled technologies.[75] Malaysia considers Autonomous Weapons Systems capable of independently selecting and attacking targets without human intervention.[76] The Philippines recognize cyberspace as the fourth dimension of warfare and priorities investment in cybersecurity facilities and personnel.[77]

The strategies for technological sovereignty range from autonomy to pragmatic cooperation. Indonesia pursues a strong and independent defense industry focusing on submarine construction, propulsion, missiles, radar, medium tanks and combat aircraft.[78] Malaysia seeks independence in selected niche areas. The country plans 10–15 per cent of the nominal offset value from Industrial Collaboration Programs for research and development.[79] The Philippines emphasizes its Self-Reliant Defence Posture Program for developing a robust defense industry maintaining AFP-developed capabilities.[80] Vietnam articulates developing self-controlled, high-tech and dual-use defense industry groups.[81] The technological choices and capabilities examined above require corresponding governance structures for effective implementation.

4.3 Dimension 3: Governance Structures and Responsibilities

The governance structures for maritime security show varying degrees of institutional integration and coordination. These structures represent what Balzacq[82] terms the "empowering audience," institutional bodies with direct causal connection to security issues and ability to enable securitizing actors. These institutional configurations translate threat perceptions into concrete organizational responses, yet their effectiveness varies significantly across the region. Singapore demonstrates a whole-of-government approach, exemplified by the coordinated multi-agency oil spill and leak responses.[83] The Digital and Intelligence Service, founded in 2022, collaborates closely with other national agencies. The joint Critical Infrastructure Defence Exercise involved about 200 front-line cyber defenders from 25 national agencies.[84] Indonesia structures coordination through the total defense system. For military threats, the Tentara Nasional Indonesia acts as the main component, supported by reserve and support components through mobilization. For non-military threats, non-defense ministries lead as main elements.[85] However, Indonesia's maritime security governance exemplifies coordination challenges through its coast guard agency, Bakamla. Despite Law No. 32/2014 granting Bakamla broad enforcement mandate and formally establishing it as the central maritime security authority, the agency encounters significant institutional resistance from other agencies and ministerial bodies, reflecting persistent *sector egos* and resource competition.[86]

Malaysia established the Joint Forces Headquarters in 2004 for coordinating joint operations among the three armed forces branches. The Ministry of Defence collaborates closely with the National Cyber Security Agency. The MAF Cyber Defence Operation Centre partners strategically with the National Cyber Coordination and Command Centre.[87] The Philippines utilizes the National Coast Watch Centre to consolidate cross-sector efforts. The Area Task Force North serves as an existing coordination mechanism for maritime security. The strategy emphasizes convergence among the AFP, PNP and local government units within the whole-of-government approach.[88] Vietnam displays a differentiated distribution with the navy as the core service for sovereignty protection. The Coast Guard

acts as a specialized state force for law enforcement and maritime national security protection. The Border Guard manages national borders on land, sea and islands.[89]

The civil-military interfaces are defined and operationalized differently across the countries studied: Malaysia distinguishes clearly the Malaysian Maritime Enforcement Agency for maritime security threats from military forces for defense tasks. The military supports civilian authorities' law enforcement with clear escalation thresholds through differentiated primary and secondary armed forces roles.[90] Vietnam defines precise roles for its maritime forces. The Coast Guard conducts maritime safety, order and security control, and law enforcement activities.[91]

Public-private partnerships develop differently across the region. Singapore leads with the Maritime Cyber Assurance and Operations Centre, a joint MPA-industry cyber security operations center with 10 companies from various maritime sectors. The Maritime Cybersecurity Roundtable, initiated by the Singapore Shipping Association with MPA and industry participation, strengthens the industry's cybersecurity capabilities.[92] Malaysia plans incentive structures for private security investments through a Defence Investment Committee chaired by the prime minister.[93]

The legal frameworks rest on the UN Convention on the Law of the Sea of 1982 as the international foundation. National approaches vary considerably. Indonesia references Law No. 3 of 2002 on National Defence and aligns national legislation with international legal norms based on democratic and human rights principles.[94] The Philippines emphasize the 2016 Arbitration Award as the legal basis for Philippine sovereign rights over waters in the West Philippine Sea.[95] These government arrangements ultimately shape how states engage in regional cooperation mechanisms.

4.4 Dimension 4: Regional Cooperation Mechanisms

The regional cooperation preferences show a balanced picture combining bilateral and multilateral approaches. The *ASEAN Maritime Outlook* favors multilateral formats with numerous regional forums and mechanisms. Bilateral cooperation complements this, as shown by the trilateral maritime patrol between Indonesia, Malaysia and the Philippines in the Sulu Sea.[96] Indonesia maintains extensive bilateral cooperation with all ASEAN states, including the General Border Committee with Malaysia since 1972. ASEAN's centrality as a regional organization remains crucial for regional integration.[97] Malaysia articulates a balanced approach, noting that bilateralism and multilateralism operate together. The country maintains strategic partnerships with 16 countries and comprehensive partnerships with 11 countries. Concrete mechanisms such as the Malacca Straits Patrol and the Trilateral Cooperative Arrangement are mentioned as successful cooperation models.[98] The Philippines participates actively in the Trilateral Cooperation Agreement with Malaysia and Indonesia against extremist and terrorist border movements.[99] Malaysia and the Philippines affirm ASEAN centrality as foreign policy cornerstone, though the Philippines acknowledge limitations from economic disparities among members hindering a true ASEAN community.[100]

The balance of sovereignty and cooperation depth remains a key challenge for all participating states. Vietnam articulates the most restrictive position with its four-no policy: no military alliances, no taking sides for one country against another, no permission

for foreign military bases or Vietnamese territorial use for military activities against neighboring states.[101] The Vietnamese position reflects the challenge of securitization as an "intersubjective process" requiring mutual recognition between actors while respecting distinct national contexts.[102] Indonesia emphasizes respect for national sovereignty, non-interference in internal affairs and mutual benefit as basic cooperation principles.[103] Malaysia shows greater flexibility through the Trilateral Cooperative Arrangement, allowing pursuit beyond maritime borders and establishing a transit corridor for ships.[104]

External partner involvement reflects regional great power competition. The Philippines highlight the USA as the only treaty ally through the 1951 RP-US Mutual Defence Treaty and the 2014 Enhanced Defense Cooperation Agreement (EDCA). EDCA priorities explicitly include maritime security and maritime domain awareness.[105] Indonesia describes the US as a strategic partner for developing institutional capacity, operational capability, human resource professionalism and weapon system modernization.[106] Malaysia warns of regional polarization risks from a rivalry among powerful nations.[107] China receives ambivalent assessment. The Philippines Defence White Paper characterizes China's ongoing activities in the South China Sea as a significant security threat.[108] Indonesia describes China as a strategic partner aligned with Indonesian national interests for defense capability building.[109] Vietnam notes sovereignty-related differences regarding the East Sea as historically rooted.[110] Singapore maintains careful balance, emphasizing national autonomy. The government, MINDEF and SAF operate without assuming dependence on external rescue.[111]

The preceding dimensional analysis reveals both convergent patterns and persistent divergences that shape the regional security landscape. These findings now require a synthesis to understand their collective implications for maritime infrastructure protection.

V. Synthesis: Maritime Security of Critical Infrastructure in Southeast Asia

The systematic analysis of national defense white papers from Southeast Asia reveals a heterogeneous picture of strategies for protecting critical maritime infrastructure.

5.1 Converging Threat Perceptions with Different Priorities

All analyzed states recognize great power competition as a structural challenge, demonstrating Balzacq's[112] concept of intersubjective securitization through mutually constituted threat understandings. However, this common assessment leads to different national priority-setting. The Philippines perceives the territorial conflict in the South China Sea as an immediate threat to their existence, while Malaysia voices concern about the transformation of the region into a geopolitical playing field. Vietnam and Indonesia choose more abstract formulations. These rhetorical differences reflect different degrees of direct concern and different foreign policy positions vis-à-vis the major powers, especially China. Indonesia explicitly characterizes hybrid threats as a fusion of military and non-military elements. The Philippines link territorial conflicts with environmental

degradation. These conceptual differences have an impact on the development of national counterstrategies and make the regional coordination of protective measures more difficult.

5.2 Technological Asymmetries

The technological security approaches of the countries analyzed show asymmetries. Singapore plays a pioneering role with the world's first Maritime Digital Twin and AI-supported cyber security systems. The ReCAAP Information Sharing Centre exemplifies Singapore-based regional information sharing through its web-based reporting and analysis portal for piracy and robbery incidents.[113] Vietnam, on the other hand, is concentrating on conventional deterrence capacities through submarines and coastal defense systems. This technological divide reflects different economic capacities and clear differences in strategic orientation. While Singapore favors preventive protection through technology, Vietnam pursues an approach of reactive deterrence through military strength. Surveillance, resilience and physical protection vary according to technological capacities. Singapore's integrated approach combines all three elements in one digital system. Malaysia and Indonesia develop C4ISR systems incrementally.

The different strategies for technological sovereignty are particularly revealing. Indonesia is pursuing ambitious plans for an independent defense industry with a focus on submarine construction and missile technology. Malaysia specializes in niche areas. These different paths to technological autonomy reflect different assessments of balancing national independence against the benefits of international technology cooperation.

5.3 Governance Between Integration and Fragmentation

The institutional arrangements for protecting maritime infrastructure also demonstrate different models of governmental coordination. Singapore's whole-of-government approach seamlessly integrates civilian and military actors. This integrated governance extends to digital infrastructure management. Singapore's Maritime Single Window system, currently under implementation, aims to digitize all port call and security documentation processes, though mandatory cyber security requirements remain absent.[114] In contrast to Singapore, Vietnam maintains clear functional distinctions because the Navy, Coast Guard and Border Guard have clearly defined areas of responsibility. These structural differences significantly impact the ability of the respective states to respond to hybrid threats. Private sector involvement also proves to be a decisive factor for effective infrastructure protection. This exemplifies Balzacq's[115] concept of *functional actors* who significantly influence security dynamics without being the primary securitizing actors. Singapore's Maritime Cyber Assurance and Operations Centre functions as a joint industry-government operations center and demonstrates the benefits of close cooperation. All other analyzed countries remain reluctant, limiting their capacity to leverage private expertise and resources.

5.4 Regional Cooperation Versus National Interests

States prefer multilateral formats while maintaining bilateral special relations. All states affirm ASEAN centrality, but practical implementation falls short of stated

ambitions. ASEAN's institutional architecture for maritime security reveals both structural limitations and opportunities for modular cooperation. The consensus principle significantly slows any course correction. The failed 2012 AMM communiqué on the Scarborough Shoal dispute demonstrates how internal disagreement can block institutional action.[116] Despite these limitations, ASEAN has created a structure through institutional diversification in which each forum has clearly defined functions for balancing, hedging and co-opting, which can be selected depending on the situation. The ADMM/ADMM-Plus functions, for example, as rule and capacity platforms, developing maritime behavioral codes through initiatives like CUES adoption and GAME guidelines, progressively extending these to partner states.[117] However, minilaterals show concrete successes. The Malacca Straits Patrol as well as the trilateral cooperation in the Sulu Sea function better as focused arrangements than comprehensive multilateral mechanisms.

5.5 Implications for the Research Question

Ensuring critical maritime infrastructure security in Southeast Asia remains theoretically possible through technological innovation and regional cooperation, but structural factors present significant obstacles. Technological asymmetries create unequal conditions for joint protection, reflecting Balzacq's[118] "co-dependency of agency and context in security performance." Different governance structures and understandings of sovereignty also limit the depth of possible cooperation. The analysis demonstrates that the prospects for protecting critical maritime infrastructures, as reflected in the documents, hinge on the pairing of problematizations with specified instruments and arrangements. Furthermore, great power rivalry permeates all maritime security dimensions and complicates genuinely regional solutions. The different positions of the ASEAN states vis-à-vis the major powers, from the Philippines' partnership with the US to Vietnam's equidistance, further fragment regional approaches. These conditions constrain both technological and cooperative security strategies.

VI. Conclusion

The study examined the question of how states in Southeast Asia can ensure the security of their critical maritime infrastructure in the face of hybrid threats and geopolitical challenges through a combination of technological innovation and regional cooperation. Divergent approaches persist due to technological asymmetries, competing sovereignty concepts, and strategic fragmentation, all factors that override functional pressures for coordination.

The analysis reveals that several factors are crucial. The findings indicate that outcomes are best understood through the material and organizational specification of security problematizations. In a practice-centered reading of securitization, dispositifs and procedural references explain variation in how programs are formulated across cases. Technological asymmetries demonstrate how securitization, as Balzacq[119] argues, consists of practices instantiated through different dispositifs and tools, varying according to the habitus inherited from different social fields. The technological gap therefore not only

reflects the different economic resources of the respective countries but also differences in their strategic culture and security policy orientation. Governance fragmentation and limited private sector involvement constrain infrastructure protection. The documents analyzed show a spectrum from Vietnam's restrictive four-no policy to Malaysia's willingness to engage in cross-border operations. These different concepts of sovereignty represent a structural obstacle to the development of integrated regional protection systems that cannot be overcome by technological solutions alone.

Hybrid threats redefine Southeast Asian maritime security, necessitating technological innovation, institutional reforms, and sovereignty-sensitive regional cooperation. Future research should address the question of how technological interoperability can be achieved despite different levels of development and which innovative governance models could overcome the identified obstacles to cooperation. Resolving the puzzle of divergent security approaches, this study demonstrates that the security of critical maritime infrastructure in Southeast Asia ultimately depends on overcoming not only technological gaps but also sovereignty-sensitive governance barriers that currently fragment regional cooperation.

Notes

1. Aurel Sari, *Protecting Maritime Infrastructure from Hybrid Threats: Legal Options*, Hybrid CoE Research Report 14 (Helsinki, 2025), pp. 27–32.
2. Miranda Bryant, "Spy Ships, Cyber-Attacks and Shadow Fleets: The Crack Security Team Braced for Trouble at Sea," *The Guardian*, June 18, 2025, https://www.theguardian.com/environment/2025/jun/18/shadow-fleets-cyber-attacks-and-spy-ships-the-crack-security-team-braced-for-trouble-at-sea-nordic-maritime-cyber-resilience-center, accessed July 15, 2025.
3. Christian Bueger and Tobias Liebetrau, "Critical Maritime Infrastructure Protection: What's the Trouble?" *Marine Policy* 155 (2023), p. 3, https://doi.org/10.1016/j.marpol.2023.105772.
4. Meixuan Li, Jianying Zhou, Sudipta Chattopadhyay, and Mark Goh, "Maritime Cybersecurity: A Comprehensive Review," *Journal of Marine Science and Engineering* 12(6) (2024), p. 919, https://doi.org/10.3390/jmse12060919.
5. Rainer Jungwirth, Hanna Smith, Etienne Willkomm, Jukka Savolainen, Marina Alonso Villota, Maxime Lebrun, Aleksi Aho, and Georgios Giannopoulos, *Hybrid Threats: A Comprehensive Resilience Ecosystem-Executive Summary* (Luxembourg: Publications Office of the European Union, 2023), p. 6.
6. Jungwirth et al., 2023, p. 6; Philippe Bourbeau, *On Resilience: Genealogy, Logics, and World Politics* (Cambridge: Cambridge University Press, 2018), p. 13, https://doi.org/10.1017/9781108349017.
7. Thierry Balzacq, "A Theory of Securitization: Origins, Core Assumptions, and Variants," in Thierry Balzacq, ed., *Securitization Theory: How Security Problems Emerge and Dissolve* (London: Routledge, 2011a), pp. 1–30, p. 14, https://doi.org/10.4324/9780203868508.
8. Sari, 2025, pp. 27–28.
9. David Shambaugh, *Where Great Powers Meet: America and China in Southeast Asia* (New York: Oxford University Press, 2021), pp. 82–98, 159–162, https://doi.org/10.1093/oso/9780190914974.001.0001.
10. Balzacq, 2011a, pp. 15–18.
11. Klaus Krippendorff, *Content Analysis: An Introduction to Its Methodology* (Los Angeles: SAGE Publications, 2013).
12. Christian Bueger and Timothy Edmunds, "Beyond Sea Blindness: A New Agenda for Maritime Security Studies," *International Affairs* 93(6) (2017), pp. 1293–1297, 1298–1302, https://doi.org/10.1093/ia/iix174.
13. Christian Bueger and Tobias Liebetrau, p. 3.
14. Asian Development Bank, *Disaster Resilient Infrastructure: Unlocking Opportunities for Asia and the Pacific*, Sustainable Development Working Paper Series (Manila, 2022), pp. 10ff, 18–23.
15. Brendon J. Cannon, "Undersea Cable Security in the Indo-Pacific: Enhancing the Quad's Collaborative Approach," *Marine Policy* 171 (2025), pp. 1–2, https://doi.org/10.1016/j.marpol.2024.106415.

16. Xue Wang, Debin Du, and Yan Peng, "Assessing the Importance of the Marine Chokepoint: Evidence from Tracking the Global Marine Traffic," *Sustainability* 16(1) (2024), p. 8, https://doi.org/10.3390/su16010384.

17. Boston Consulting Group, "These Four Chokepoints Are Threatening Global Trade," BCG Insights, 2024, https://www.bcg.com/publications/2024/these-four-chokepoints-are-threatening-global-trade, accessed July 15, 2025.

18. Geoffrey Till, *The Changing Maritime Scene in Asia: Rising Tensions and Future Strategic Stability* (Basingstoke: Palgrave Macmillan, 2015), pp. 3–6.

19. Sergiu Mitrescu and Martin Sokolov, "In the Crosshairs: Hybrid Threats and the Challenge to Maritime Infrastructure," in George Scutaru and Murman Margvelashvili, eds., *Defending Maritime Assets* (Dordrecht: Springer, 2025), pp. 67–68, https://doi.org/10.1007/978-94-024-2300-6_6.

20. Adam J. Fenton, "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) (2024), pp. 1–4, 13–18, https://doi.org/10.3390/jmse12030510.

21. Cynthia Mehboob and Fitriani, "Securing Our Data: Subsea Cables and Maritime Security in Southeast Asia," *Blue Security: A Maritime Affairs Series* 11 (2025), pp. 4–12.

22. Sören Scholvin and Mikael Wigell, "Geo-Economic Power Politics: An Introduction," in Mikael Wigell, Sören Scholvin, and Mika Aaltola, eds., *Geo-Economics and Power Politics in the 21st Century: The Revival of Economic Statecraft* (London: Routledge, 2019), pp. 2–4, https://doi.org/10.4324/9781351172288-1.

23. Amir Hossein Gharehgozli, Joan Mileski, Alyssa Adams, and Wyndylyn von Zharen, "Evaluating a 'Wicked Problem': A Conceptual Framework on Seaport Resiliency in the Event of Weather Disruptions," *Technological Forecasting & Social Change* 121 (2017), pp. 65–68, 69–72, https://doi.org/10.1016/j.techfore.2016.11.006.

24. Suk Kyoon Kim, "Challenges to the Capacity-Building of Maritime Domain Awareness (MDA) in East Asia: What Is at Stake?" *Ocean Development & International Law* 44(1) (2024), pp. 403–405.

25. Bueger and Edmunds, 2017, pp. 1303–1308.

26. James Kraska, "Intelligence Collection and the International Law of the Sea," *International Law Studies* 99 (2022), pp. 602–673, pp. 605–612.

27. Mizuho Kajiwara, "Underwater Competition in the Indo-Pacific," in Alexander L. Vuving, ed., *Hindsight, Insight, Foresight: Thinking About Security in the Indo-Pacific* (Asia-Pacific Center for Security Studies: Honolulu, 2020), pp. 191–208, pp. 201–205.

28. Benedetta Girardi and Julie Ebrard, "Maritime Supply Chains: Connecting Trade and Security Through Enhanced Dutch-Korean Cooperation," in *The Hague Centre for Strategic Studies, Maritime Security for Resilient Global Supply Chains in the Wider Indo-Pacific* (Den Haag: HCSS, 2024), p. 100.

29. Jeslyn Tan, "Securing the Backbone: Security Challenges to and Governance of Submarine Cables in the Indo Pacific," *Melbourne Asia Review*, 2024, https://www.melbourneasiareview.edu.au/-securing-the-backbone-security-challenges-to-and-governance-of-submarine-cables-in-the-indo-pacific/, accessed July 11, 2025.

30. Scott Edwards, "Fragmentation, Complexity and Cooperation: Understanding Southeast Asia's Maritime Security Governance," *Contemporary Southeast Asia* 44(1) (2022), pp. 95–97, 101–102, https://doi.org/10.1355/cs44-1d.

31. Kornwika Poonnawatt, "Multilateral Cooperation Against Maritime Piracy in the Straits of Malacca: From the RMSI to ReCAAP," *Marine Policy* 152 (2023), pp. 2–3, https://doi.org/10.1016/j.marpol.2023.105628.

32. Tara Maria Davenport, "The Protection of Submarine Cables in Southeast Asia: The Security Gap and Challenges and Opportunities for Regional Cooperation," *Marine Policy* 171 (2025), pp. 4–7, https://doi.org/10.1016/j.marpol.2024.106435; Poonnawatt, 2023, p. 7.

33. Davenport, 2025, p. 4.

34. Kei Koga, *Managing Great Power Politics: ASEAN, Institutional Strategy, and the South China Sea* (Singapore: Palgrave Macmillan, 2022), pp. 165–166, https://doi.org/10.1007/978-981-19-2611-2.

35. Davenport, 2025, pp. 4–7.

36. Kristi Govella, "Undersea Cables, Geoeconomics, and Security in the Indo-Pacific: Risks and Resilience," *Marine Policy* 180 (2025), p. 1, https://doi.org/10.1016/j.marpol.2025.106809.

37. *Ibid.*, p. 4.

38. James E. Platte, "Deterrence at Sea: The Maritime Domain in U.S. Deterrence Strategy in the Indo-Pacific," *The Pacific Review* (2024), pp. 8–11, https://doi.org/10.1080/09512748.2024.2444350.

39. Krippendorff, 2013, pp. 24–30.
40. Fredie Tan, "The National Security Thinking of Australia and Singapore," *The Forge*, 2020, https://theforge.defense.gov.au/article/national-security-thinking-australia-and-singapore, accessed July 14, 2025.
41. Thierry Balzacq, "Enquiries into Methods: A New Framework for Securitization Analysis," in Thierry Balzacq, ed., *Securitization Theory: How Security Problems Emerge and Dissolve* (London: Routledge, 2011b), pp. 31–53, pp. 35ff, https://doi.org/10.4324/9780203868508.
42. Krippendorff, 2013, pp. 37–45.
43. *Ibid.*, pp. 98–104.
44. *Ibid.*, pp. 333–351.
45. Balzacq, 2011a, p. 16.
46. Ministry of Defence Malaysia, *Defence White Paper: A Secure, Sovereign and Prosperous Malaysia* (Kuala Lumpur: Ministry of Defence Malaysia, 2020), p. 9.
47. Ministry of Defence of the Republic of Indonesia, *Indonesian Defence White Paper* (Jakarta: Ministry of Defence of the Republic of Indonesia, 2015), p. 24.
48. Department of National Defense, *National Defense Strategy 2018–2022* (Quezon City: Department of National Defense, 2018), p. 11.
49. Ministry of National Defence of the Socialist Republic of Viet Nam, *Viet Nam National Defence White Paper* (Hanoi: Ministry of National Defence of the Socialist Republic of Viet Nam, 2019), pp. 18–19.
50. Eng Hen Ng, "Speech by Minister for Defence at the Committee of Supply Debates 2024," *Ministry of Defence Singapore*, February 28, 2024, https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2024/February/28feb24_speech, accessed July 15, 2025.
51. Balzacq, 2011a, p. 3.
52. Ministry of Defence of the Republic of Indonesia, 2015, p. 59.
53. Ministry of Defence Malaysia, 2020, pp. 45–46.
54. Department of National Defense, 2018, p. 12.
55. Ministry of National Defence of the Socialist Republic of Viet Nam, 2019, p. 19.
56. Balzacq, 2011b, p. 35.
57. Ministry of Defence of the Republic of Indonesia, 2015, p. 9.
58. Ministry of Defence Malaysia, 2020, pp. 44ff.
59. Department of National Defense, 2018, p. 11.
60. Ministry of National Defence of the Socialist Republic of Viet Nam, 2019, p. 12.
61. Association of Southeast Asian Nations, *ASEAN Maritime Outlook* (Jakarta: ASEAN Secretariat, 2023), p. 41.
62. *Ibid.*, p. 41.
63. *Ibid.*, p. 42.
64. Balzacq, 2011a, pp. 24ff.
65. Maritime and Port Authority of Singapore, "Press Release: 19th Singapore Maritime Week Opens with Record Attendance and Industry Participation at EXPO@SMW," *MPA Singapore*, March 24, 2025, https://www.mpa.gov.sg/media-center/details/19th-singapore-maritime-week-opens, accessed July 16, 2025.
66. Maritime and Port Authority of Singapore, *Annual Report 2024* (Singapore: MPA, 2024), https://www.mpa.gov.sg/web/wcm/connect/www/fb6c4b8c-annual-report-2024.pdf, accessed July 16, 2025, pp. 17–21.
67. Ministry of National Defence of the Socialist Republic of Viet Nam, 2019, p. 84.
68. Ministry of Defence Malaysia, 2020, pp. 48ff.
69. Ministry of Defence of the Republic of Indonesia, 2015, p. 2, p. 9.
70. Department of National Defense, 2018, p. 58.
71. Balzacq, 2011a, p. 20.
72. Maritime and Port Authority of Singapore, "Press Release: 19th Singapore Maritime Week Opens with Record Attendance and Industry Participation at EXPO@SMW."
73. Ministry of Defence Malaysia, 2020, pp. 49, 52.
74. Department of National Defense, 2018, p. 32.
75. Maritime and Port Authority of Singapore, "Media Release: Collective Efforts to Strengthen Maritime Cybersecurity."
76. Ministry of Defence Malaysia, 2020, p. 27.
77. Department of National Defense, 2018, pp. 17, 45.

78. Ministry of Defence of the Republic of Indonesia, 2015, pp. 46–47, p. 71.
79. Ministry of Defence Malaysia, 2020, p. 83.
80. Department of National Defense, 2018, p. 36.
81. Ministry of National Defence of the Socialist Republic of Viet Nam, 2019, p. 39.
82. Balzacq, 2011a, p. 10.
83. Maritime and Port Authority of Singapore, p. 11.
84. Eng Hen Ng, "Speech by Minister for Defence at the Committee of Supply Debates 2024."
85. Ministry of Defence of the Republic of Indonesia, 2015, p. 31.
86. Dedi Dinarto, "Can Bakamla Be at the Forefront of Indonesia's Natuna Sea Strategy?" *IDSS Paper No. 002/2022* (Singapore: S. Rajaratnam School of International Studies [RSIS], 2022).
87. Ministry of Defence Malaysia, 2020, pp. 15, 26.
88. Department of National Defense, 2018, pp. 44, 15.
89. Ministry of National Defence of the Socialist Republic of Viet Nam, 2019, pp. 67, 83ff.
90. Ministry of Defence Malaysia, 2020, pp. 27, 50.
91. Ministry of National Defence of the Socialist Republic of Viet Nam, 2019, pp. 83, 67.
92. Maritime and Port Authority of Singapore, "Media Release: Collective Efforts to Strengthen Maritime Cybersecurity."
93. Ministry of Defence Malaysia, 2020, p. 83.
94. Ministry of Defence of the Republic of Indonesia, 2015, p. 53.
95. Department of National Defense, 2018, p. 12.
96. Association of Southeast Asian Nations, 2023, p. 9.
97. Ministry of Defence of the Republic of Indonesia, 2015, pp. 78–82, 95.
98. Ministry of Defence Malaysia, 2020, pp. 23–24, pp. 64–74.
99. Department of National Defense, 2018, pp. 23, 46.
100. Ministry of Defence Malaysia, 2020, p. 24.
101. Department of National Defense, 2018, p. 22.
102. Balzacq, 2011a, p. 3.
103. Ministry of Defence of the Republic of Indonesia, 2015, pp. 77–78.
104. Ministry of Defence Malaysia, 2020, p. 72.
105. Department of National Defense, 2018, p. 21.
106. Ministry of Defence of the Republic of Indonesia, 2015, p. 88.
107. Ministry of Defence Malaysia, 2020, p. 21.
108. Department of National Defense, 2018, pp. 23, 11.
109. Ministry of Defence of the Republic of Indonesia, 2015, p. 83.
110. Ministry of National Defence of the Socialist Republic of Viet Nam, 2019, p. 16.
111. Eng Hen Ng, "Speech by Minister for Defence at the Committee of Supply Debates 2024."
112. Balzacq, 2011a, p. 3.
113. Fenton, 2024, p. 16.
114. *Ibid.*, p. 21.
115. Balzacq, 2011b, p. 35.
116. Koga, 2022, pp. 165–168.
117. *Ibid.*, pp. 163–164, pp. 214–220.
118. Balzacq, 2011a, p. 16.
119. *Ibid.*, p. 18.

Biographical Statement

Deniz Kocak is a research associate at the Helmut Schmidt University / University of the Federal Armed Forces Hamburg and is affiliated with the Interdisciplinary Research Focus Maritime Security (iFMS), specializing in Indo-Pacific security governance.

Submitted: 07-22-2025 • Sent for Review: 08-21-2025 • Sent for Revision: 10-07-2025 • Resubmitted: 10-23-2025 • Sent for Revision: 10-30-2025 • Decision: 11-12-2025