

Modeling Smart Defense for Indonesia's Archipelagic Maritime Defense Strategy: A System Dynamics Approach

Joko Purnomo, Okol Sri Suharyo, Sutikno Wahyu Hidayat, Eko Krisdiono
Sekolah Tinggi Teknologi Angkatan Laut, Surabaya, Indonesia

ABSTRACT

This study aims to analyze the influence of price perception and brand image on the purchasing decisions for Glad2Glow skincare products among students of the Entrepreneurship Study Program at Universitas Negeri Makassar. The study employs a quantitative approach with a sample of 84 respondents selected using purposive sampling. Data collection was conducted via questionnaires, while data analysis utilized multiple linear regression with the aid of SPSS version 30. The results indicate that price perception and brand image each have a positive and significant partial effect on purchasing decisions. Simultaneously, both variables also exert a positive and significant influence on purchasing decisions for Glad2Glow skincare products. The coefficient of determination value of 90.8% indicates that purchasing decisions can be explained by price perception and brand image, while the remaining 9.2% is influenced by factors outside the scope of this study. These findings demonstrate that the more favorable the perception of price and brand image regarding Glad2Glow, the higher the likelihood of students purchasing the product.

Keywords: Price Perception, Brand Image, Purchase Decision, Glad2Glow

Corresponding author

Name: Joko Purnomo

Email: jokopurnomo.sttal@yahoo.com

INTRODUCTION

Indonesia is the world's largest archipelagic state, strategically positioned between the Asian and Australian continents and between the Pacific and Indian Oceans. This geographical position places Indonesia at the intersection of major international maritime trade and shipping routes connecting the Asia-Pacific region with the Middle East, Africa, and Europe. Consequently, Indonesian waters have substantial strategic value for national economic activity, international maritime transportation, and regional security. At the same time, the country's extensive maritime territory creates a complex defense environment that requires continuous surveillance, effective maritime presence, and the ability to respond to both conventional and non-conventional threats. The strategic importance of Indonesia's maritime domain therefore requires a defense strategy that is adaptive, integrated, and capable of responding to the dynamic characteristics of the maritime environment.

The Indonesian Navy has an important role in maintaining national sovereignty, maritime security, and the protection of national interests at sea. In carrying out these responsibilities, the Indonesian Navy operates within the framework of the Archipelagic

Maritime Defense Strategy (SPLN), which requires the integration of naval forces, operational capabilities, surveillance systems, supporting infrastructure, and human resources. The development of Indonesia's maritime defense has traditionally emphasized the strengthening of the Integrated Fleet Weapon System (SSAT), consisting of warships, naval aircraft, marine forces, and naval bases. However, the increasingly complex maritime environment requires these capabilities to be developed not only in terms of physical strength but also through greater integration of information, technology, operational concepts, and decision-making processes.

The changing character of contemporary security threats further reinforces this requirement. Maritime threats are no longer limited to conventional military confrontation but also include maritime violence, illegal activities, smuggling, illegal fishing, illegal mining, environmental threats, navigation-related risks, and cyber-related threats. At the same time, technological developments have fundamentally changed the conduct of military operations. Information and communication technologies, network-centric operations, Intelligence, Surveillance and Reconnaissance (ISR), Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance, artificial intelligence, big data, machine learning, and autonomous systems have increasingly become important components of modern defense capability (Darajati & Syafei, 2022; Bueger & Edmunds, 2020; Ben Farah et al., 2022; Bolbot et al., 2022; Akdağ et al., 2022; Taddeo et al., 2021). These developments require defense organizations to move beyond conventional approaches and develop integrated capabilities that can transform information and technology into operational advantages.

In this context, Smart Defense provides an important strategic approach for improving defense capability through the effective integration of resources, technology, organizational capabilities, and operational functions. Recent maritime security research emphasizes integrated capability development, cooperation, resilience, and coordinated responses to complex and evolving threats (Bueger et al., 2020; Pertiwi, 2020; Canepa et al., 2021). Within the maritime domain, this perspective is particularly relevant because the Indonesian Navy must operate across a geographically extensive maritime area while simultaneously responding to diverse and continuously changing threats. Therefore, Smart Defense should not be interpreted merely as the acquisition of advanced technology, but rather as an integrated capability involving technology, operational strategy, force posture, and threat awareness.

The development of Smart Defense for Indonesia's maritime defense requires consideration of several interconnected dimensions. Based on the preliminary identification and expert assessment conducted in this study, four principal dimensions influence Smart Defense within the Archipelagic Maritime Defense Strategy: Technology, Operational Strategy, Indonesian Navy Posture, and Threat Perception. The Technology dimension concerns the utilization and integration of information technologies, surveillance systems, big data, cyber capabilities, artificial intelligence, machine learning, and autonomous systems. The Operational Strategy dimension concerns the ability to plan, coordinate, control, and conduct military operations, including command and control, surveillance, sea control, coastal defense, logistics, and other operational capabilities. The Indonesian Navy Posture dimension represents the readiness and configuration of naval capabilities required to perform military, constabulary, and

diplomatic roles. Meanwhile, Threat Perception represents the ability to recognize and respond to the changing spectrum of maritime threats, including emerging maritime cyber-security threats.

The four dimensions cannot be considered independently because changes in one dimension may influence the performance of the others. For example, improvements in an integrated information system can strengthen surveillance and information processing, which subsequently improves command and control and operational decision-making. Similarly, strengthening the SSAT can increase naval operational capability and contribute to improved maritime security. Conversely, increasing maritime cyber-security threats may negatively influence overall defense capability if improvements in cyber protection and resilience do not keep pace with the changing threat environment. This interdependence indicates that Smart Defense represents a complex system characterized by interactions, feedback relationships, and changes over time. Consequently, a static assessment of individual variables may not adequately capture the dynamic behavior of Smart Defense within the Indonesian maritime defense system.

Recent studies have examined maritime defense and security from several complementary perspectives, including maritime security governance, cybersecurity, autonomous systems, and maritime capability resilience. These studies demonstrate the increasing complexity of the maritime operating environment and the need to integrate technological, operational, and security dimensions (Bolbot et al., 2022; Bueger et al., 2020; Liu et al., 2022; Schinas & Metzger, 2023). However, the integration of multiple defense dimensions into a quantitative dynamic model remains relatively limited, particularly in the context of Indonesia's Archipelagic Maritime Defense Strategy.

A further methodological challenge concerns the transformation of qualitative expert knowledge into an integrated quantitative representation. Maritime defense involves strategic and operational variables that are difficult to measure directly and frequently depend on expert judgment. Therefore, identifying the most influential criteria requires a structured expert-based approach. The Delphi method can be used to obtain consensus among experts and to reduce a broad set of potential variables into the most relevant dimensions. Fuzzy Weighting can subsequently be employed to translate expert judgments and linguistic assessments into quantitative priority values. The combination of these approaches provides a systematic basis for determining the relative importance of the dimensions and variables that constitute Smart Defense.

However, determining the relative importance of variables alone is insufficient because maritime defense capabilities evolve continuously over time. Changes in technology, operational resources, force posture, and threat conditions can produce cumulative effects and feedback relationships that cannot be adequately represented through a static analytical model. Therefore, System Dynamics is employed in this study to represent the relationships among the principal Smart Defense dimensions and to examine their behavior over a five-year projection period. System Dynamics enables the representation of causal relationships, stocks, flows, feedback mechanisms, and dynamic changes, providing a suitable framework for analyzing complex maritime systems and evaluating alternative policy scenarios (Tai et al., 2021). The integration of Delphi, Fuzzy

Weighting, and System Dynamics consequently provides a methodological framework for transforming expert knowledge into a dynamic decision-support model.

Accordingly, this study aims to develop and analyze a Smart Defense model for Indonesia's Archipelagic Maritime Defense Strategy in supporting Indonesian Navy missions. Specifically, the study seeks to: (1) identify the principal dimensions and variables influencing Smart Defense; (2) determine the relative importance of these dimensions using the Delphi and Fuzzy Weighting approaches; (3) develop a System Dynamics model representing the interaction among Technology, Operational Strategy, Indonesian Navy Posture, and Threat Perception; and (4) evaluate alternative policy scenarios to identify variables that provide the greatest potential contribution to Smart Defense capability. The study contributes to the literature by integrating expert-based assessment and dynamic modeling into a single analytical framework for maritime defense. Practically, the resulting model is expected to support strategic decision-making by identifying priority areas for strengthening integrated systems, logistics, naval force posture, and maritime cyber-security capabilities within Indonesia's maritime defense strategy.

LITERATURE REVIEW

Sea Power and Archipelagic Maritime Defense

The concept of sea power provides an important theoretical foundation for understanding maritime defense in an archipelagic state. In the Indonesian context, maritime strategic geography, sea lanes, and the country's position within the Indo-Pacific are central considerations for maritime defense planning (Pertiwi, 2020). These factors determine the strategic importance of developing maritime capabilities, maintaining maritime communications, and sustaining effective presence at sea. For Indonesia, these considerations are particularly relevant because its geographical configuration consists of thousands of islands, extensive maritime jurisdiction, strategic sea lanes, and several maritime chokepoints connecting the Indian and Pacific Oceans.

The Indonesian maritime defense environment requires a defense strategy that is capable of integrating geographical characteristics with naval capabilities and operational requirements. Within this context, the Archipelagic Maritime Defense Strategy (Strategi Pertahanan Laut Nusantara/SPLN) provides a strategic framework for organizing maritime defense in accordance with Indonesia's geographical characteristics, strategic environment, and national defense resources. Recent research on Indonesia's maritime position emphasizes the strategic importance of its maritime domain within the changing Indo-Pacific environment (Pertiwi, 2020), while maritime security scholarship highlights the need for integrated capabilities, cooperation, and capacity development (Bueger et al., 2020). The implementation of SPLN consequently requires not only adequate naval forces but also effective deployment, information systems, logistics, command and control, intelligence, surveillance, and technological capabilities.

The development of naval power must therefore be understood as a multidimensional process. Naval strength cannot be assessed solely from the number of ships or weapon systems available, because operational effectiveness also depends on the ability to integrate platforms, personnel, information, logistics, command structures, and deployment patterns. Research on maritime logistics and cyber-resilience similarly

demonstrates that operational capability depends on the integration of supporting systems, information, and organizational preparedness (Canepa et al., 2021; Tai et al., 2021). These perspectives indicate that maritime defense capability is an interconnected system rather than a collection of independent assets.

Accordingly, the present study adopts an integrated perspective of maritime defense in which technological capability, operational strategy, naval force posture, and the perception of maritime threats are considered interconnected components. This perspective provides the theoretical foundation for examining Smart Defense as a capability-development approach for supporting Indonesia's archipelagic maritime defense strategy.

Smart Defense and Integrated Defense Capability

Smart Defense in the present study is conceptualized as an integrated defense-capability approach in which technological innovation, organizational preparedness, operational effectiveness, and resilience are developed together. This perspective is consistent with contemporary maritime security research emphasizing coordinated capacity building and integrated responses to complex security environments (Bueger et al., 2020; Taddeo et al., 2021). The concept is particularly relevant to maritime defense because capability development must remain effective despite changing threats, technological disruption, and resource constraints.

From a resource-management perspective, contemporary maritime defense requires the prioritization and integration of capabilities rather than isolated acquisition. Maritime capacity-building research emphasizes cooperation, institutional coordination, and the development of complementary capabilities, while cybersecurity research highlights the need for organizational preparedness and resilience alongside technical measures (Bueger et al., 2020; Drazovich et al., 2021). Smart Defense is therefore treated in this study as a managerial and operational approach for aligning available resources with changing defense requirements.

Technology nevertheless represents an important component of Smart Defense. Contemporary research highlights the increasing role of integrated information systems, autonomous systems, artificial intelligence, machine learning, and advanced navigation technologies in maritime operations (Akdağ et al., 2022; Burmeister & Constapel, 2021; Liu et al., 2022; Taddeo et al., 2021; Vagale et al., 2021; Zhang et al., 2021; Ziajka-Poznańska & Montewka, 2021). The increasing application of networked systems, cyber capabilities, big data, artificial intelligence, machine learning, autonomous systems, and integrated monitoring has transformed the manner in which military organizations collect information, assess threats, coordinate operations, and respond to rapidly changing situations. In this sense, technological integration provides an important foundation for the development of Smart Defense.

However, a technology-centered perspective alone is insufficient. Advanced technology will not necessarily produce superior defense outcomes when it is not supported by appropriate operational strategies, force posture, human resources, logistics, command and control, and organizational readiness. The present study therefore conceptualizes Smart Defense as an integrated capability consisting of four principal dimensions: Technology, Operational Strategy, Indonesian Navy Posture, and

Threat Perception. These dimensions were subsequently examined through expert assessment and quantitative weighting in order to identify their relative importance within the Smart Defense system.

The Technology dimension encompasses integrated systems, monitoring, cyber capability, Big Data, Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning, and autonomous capabilities. The Operational Strategy dimension includes command and control, coastal surveillance, mobile surveillance, coastal defense, integrated air defense, anti-submarine warfare, sea control, human-resource development, risk management, and logistics. The Indonesian Navy Posture dimension encompasses the Integrated Fleet Weapon System (Sistem Senjata Armada Terpadu/SSAT), security, defense, maritime intelligence, diplomacy, defense-area empowerment, supporting capabilities, and deployment patterns. Meanwhile, the Threat Perception dimension represents changing maritime security conditions, particularly maritime cyber-security threats.

This multidimensional interpretation is important because the four dimensions are mutually dependent. For example, technological integration can improve surveillance and command and control, but its operational benefits depend on appropriate force posture and logistics. Similarly, increasing threat perception can improve strategic awareness, but a growing threat without corresponding capability development may place additional pressure on the overall defense system. Smart Defense should therefore be understood as an integrated capability system whose performance emerges from the interaction among its component dimensions.

System Dynamics in Maritime Defense Decision Making

Complex maritime defense problems are characterized by interdependence, feedback, accumulation, delays, and changes over time. These characteristics create limitations for analytical approaches that treat defense variables as independent and static factors. System Dynamics provides an alternative approach by representing a complex system through causal relationships, feedback structures, stocks, flows, and auxiliary variables. Recent maritime applications demonstrate that System Dynamics can support the analysis of interconnected operational and resource variables and can be used to evaluate policy effects over time (Tai et al., 2021).

The application of System Dynamics is particularly relevant to defense capability development because changes in one capability may generate indirect effects on other components of the system. An increase in technological capability, for example, may improve information availability and surveillance effectiveness, which can subsequently influence command and control and operational performance. Similarly, improvements in naval posture may increase operational readiness and maritime presence, while changes in perceived threats may influence resource allocation and capability-development priorities. Such relationships create feedback mechanisms that cannot be adequately represented through a static assessment.

Previous research has demonstrated the applicability of System Dynamics to complex maritime and resource-management problems. Tai et al. (2021), for example, applied System Dynamics to port production and operation, demonstrating its usefulness for examining interconnected variables and policy effects over time. This

methodological perspective is relevant to the present study because Smart Defense similarly involves multiple interacting variables whose effects evolve dynamically. The System Dynamics approach therefore provides a suitable basis for decision support in maritime defense planning.

For the present study, System Dynamics is used to represent Smart Defense as the aggregate outcome of four interacting dimensions. The model incorporates Technology, Operational Strategy, Indonesian Navy Posture, and Threat Perception into a dynamic structure that allows their relationships and changes to be examined over time. This approach makes it possible not only to determine the relative importance of each dimension but also to examine how changes in specific variables influence the overall Smart Defense capability.

The use of System Dynamics also provides a basis for evaluating alternative policy interventions. Instead of asking only which variable has the highest current priority, the model enables decision makers to examine how strengthening particular capabilities may affect Smart Defense over a defined period. This is particularly relevant for defense planning because investment decisions, force modernization, technological development, and operational improvements generally produce effects that accumulate over time rather than immediately.

Research Gap and Conceptual Framework

The literature reviewed above indicates several important limitations in previous research on Smart Defense and maritime defense capability. Recent studies have expanded knowledge on maritime cybersecurity, maritime security capacity building, autonomous systems, and cyber-resilience, but these strands of research tend to address particular components of the maritime defense system separately (Afenyo & Caesar, 2023; Bolbot et al., 2022; Bueger et al., 2020; Schinas & Metzger, 2023). Although these studies provide important foundations, they do not explicitly quantify the interaction among technology, operational strategy, naval force posture, and threat perception within an integrated maritime defense framework.

Second, recent research in the Indonesian and broader maritime context has addressed maritime strategic positioning, security governance, logistics, and cyber-resilience, but these contributions generally focus on particular components of maritime capability (Pertwi, 2020; Canepa et al., 2021; Bueger et al., 2020). Other studies have examined technological and cybersecurity dimensions, including autonomous systems and cyber risk assessment (Park et al., 2023; Kanwal et al., 2022). However, these contributions do not fully integrate technological capability, operational effectiveness, naval posture, and changing threat conditions into a single dynamic Smart Defense framework.

Third, the assessment of defense capability frequently involves expert knowledge because several strategic and operational variables cannot be measured directly using conventional quantitative indicators. Expert judgment is therefore important for identifying relevant variables and determining their relative importance. However, qualitative expert judgments need to be systematically transformed into quantitative information if they are to support prioritization and policy analysis. The present study addresses this issue by applying the Delphi method to obtain expert

consensus regarding the principal dimensions and variables of Smart Defense, followed by Fuzzy Weighting to transform expert assessments into quantitative priority weights.

Fourth, a static assessment of defense capability is also insufficient for a maritime defense environment characterized by continuous technological development, changing operational requirements, force modernization, and evolving security threats. Improvements in one capability may influence other components of the defense system and may generate effects that accumulate over time. For example, improved technological integration may strengthen surveillance and command and control, which can subsequently improve operational effectiveness. Similarly, changes in threat perception may influence capability-development priorities and resource allocation. These interdependencies indicate the need for an analytical approach capable of representing feedback relationships and changes in system behavior over time.

To address these limitations, this study develops a conceptual framework in which Smart Defense is positioned as an integrated maritime defense capability resulting from the interaction of four principal dimensions: Technology, Operational Strategy, Indonesian Navy Posture, and Threat Perception. These four dimensions were identified from the theoretical and empirical literature and subsequently examined through expert assessment. Rather than treating the dimensions as isolated factors, the framework assumes that their interaction contributes to the overall effectiveness of Smart Defense in supporting Indonesian Navy missions.

The Technology dimension represents the technological foundation required to support integrated maritime defense. It includes integrated information systems, monitoring and surveillance systems, cyber capability, Big Data, Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning, and autonomous systems. The Operational Strategy dimension represents the ability to translate available capabilities into effective maritime operations and includes command and control, coastal surveillance, mobile surveillance, coastal defense, integrated air defense, anti-submarine warfare, sea control, human-resource development, risk management, and logistics. The Indonesian Navy Posture dimension represents the organization, readiness, deployment, and supporting capabilities of the naval force, including the Integrated Fleet Weapon System (SSAT), security, defense, maritime intelligence, naval diplomacy, defense-area empowerment, supporting capabilities, and deployment patterns. The Threat Perception dimension represents the changing maritime security environment, including conventional and non-conventional threats and maritime cyber-security threats.

The framework also recognizes that Smart Defense operates within a broader strategic environment. National interests, the geopolitical environment, the strategic value of the maritime domain, and limitations in available resources constitute important external drivers that influence defense capability development. These drivers provide the contextual conditions within which the four principal dimensions interact. Consequently, Smart Defense is conceptualized not simply as the accumulation of technological assets or military platforms, but as an integrated capability that depends on the alignment of technology, operational strategy, naval posture, and awareness of changing threats.

Figure 1 presents the conceptual framework of the study. The four principal dimensions converge on Smart Defense as the central capability outcome. The

framework further connects Smart Defense with expected outcomes, including stronger maritime defense capability, more effective Indonesian Navy missions, improved maritime security, and better protection of national interests. This relationship emphasizes that Smart Defense is ultimately intended to strengthen the ability of the Indonesian Navy to perform its missions within the country's complex maritime environment.

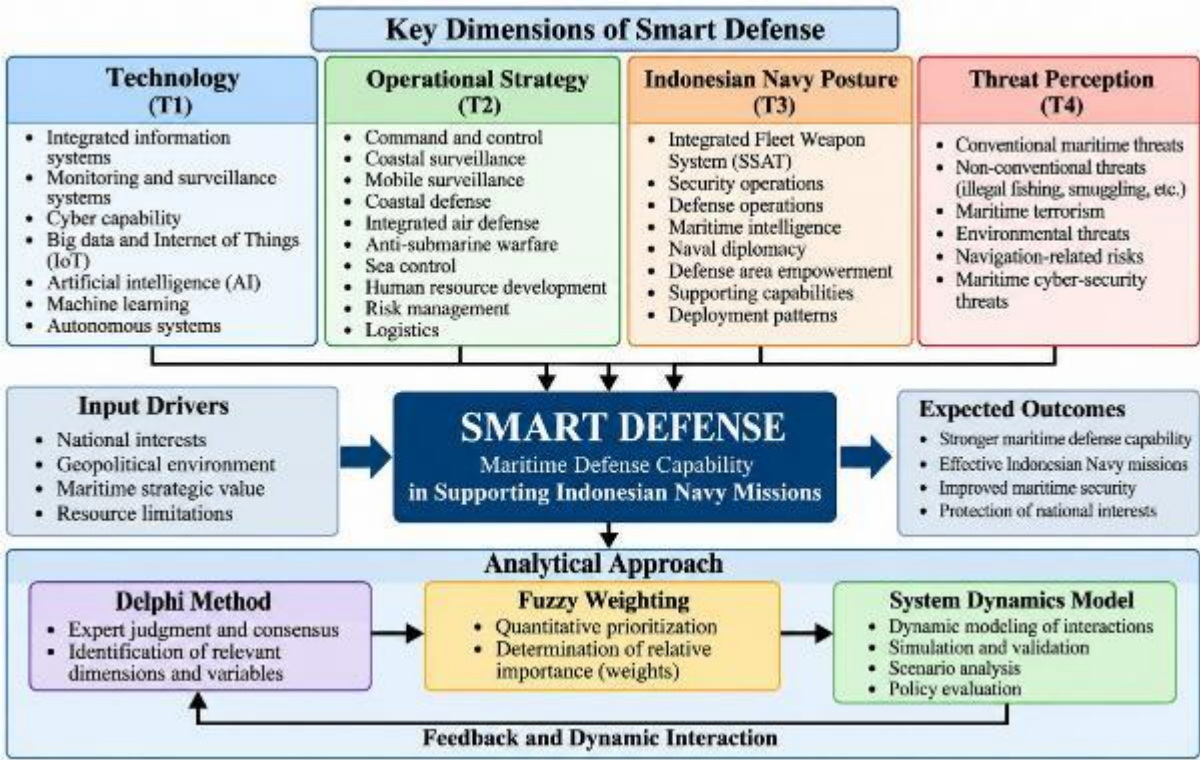


Figure 1. Conceptual Framework of Smart Defense for Indonesia's Archipelagic Maritime Defense Strategy

The lower part of Figure 1 illustrates the analytical approach used to operationalize the conceptual framework. The Delphi method is applied to obtain expert consensus and identify the dimensions and variables that are considered relevant to Smart Defense. The identified variables are subsequently processed using Fuzzy Weighting to determine their relative importance and convert expert judgments into quantitative priority weights. These weights are then incorporated into a System Dynamics model, which represents the interactions among the variables, feedback mechanisms, changes over time, and alternative policy interventions.

The integration of these three analytical stages provides a systematic pathway from expert knowledge to dynamic policy analysis. Delphi establishes the substantive relevance of the variables, Fuzzy Weighting provides their quantitative prioritization, and System Dynamics represents how the resulting capability structure may evolve over time. This integrated approach is particularly appropriate because Smart Defense involves multiple interacting dimensions whose effects cannot be adequately represented through a static or single-variable analysis.

The conceptual framework therefore provides the foundation for the empirical and modeling stages of this study. The subsequent methodology operationalizes the framework through a sequential process consisting of expert assessment, Delphi-based variable selection, Fuzzy Weighting, System Dynamics model development, model verification and validation, sensitivity analysis, and policy scenario analysis. Through this process, the study seeks to move beyond a predominantly conceptual understanding of Smart Defense toward a quantitative and dynamic framework that can support maritime defense capability planning and decision-making.

Positioning of the Present Study

The literature review establishes that the novelty of this study does not lie merely in introducing the concept of Smart Defense. Rather, its contribution lies in integrating four dimensions of maritime defense capability into a quantitative dynamic framework and combining Delphi, Fuzzy Weighting, and System Dynamics to evaluate their interaction over time. The framework consequently moves from a predominantly conceptual discussion of Smart Defense toward a measurable and policy-oriented model for Indonesian maritime defense decision-making.

RESEARCH METHODOLOGY

Research Design

This study employed a sequential mixed-method research design that combined qualitative expert elicitation with quantitative prioritization and System Dynamics modeling. The research was designed to address the multidimensional and dynamic characteristics of Smart Defense within Indonesia's Archipelagic Maritime Defense Strategy (SPLN). The methodological process consisted of several sequential stages: identification of relevant variables through literature review and field investigation; expert assessment using the Delphi method; quantitative prioritization using Fuzzy Weighting; development of a System Dynamics model; model verification and validation; sensitivity analysis; and policy scenario analysis.

The sequential structure was selected because no single analytical method was considered sufficient to address the research problem. Expert knowledge was required to identify and validate the dimensions relevant to Smart Defense, while Fuzzy Weighting was required to transform qualitative expert judgments into quantitative priorities. System Dynamics was subsequently applied to represent the interactions among the identified variables and to examine their behavior over time. The overall research procedure therefore established a methodological link between expert knowledge, quantitative weighting, and dynamic policy analysis.

The research process can be summarized as follows:

Literature Review and Field Investigation → Expert Identification → Delphi Assessment → Fuzzy Weighting → System Dynamics Model Development → Verification and Validation → Sensitivity Analysis → Policy Scenario Analysis

The System Dynamics model was developed and simulated using Stella 9.1.3, with a five-year projection interval covering 2023–2028. This interval was used to

examine the development of Smart Defense capability and the potential effects of alternative policy interventions over time.

Data Sources and Expert Participants

The study utilized both primary and secondary data. Primary data were obtained through field observation, in-depth interviews, and structured questionnaires administered to experts with relevant responsibilities and knowledge of Indonesian maritime defense. Secondary data were obtained from defense regulations, strategic documents, books, scientific journal articles, and other relevant institutional documents.

The expert assessment involved seven Indonesian Navy officials representing different functional areas associated with maritime defense capability. The expert panel included representatives from security and cryptography, naval education, naval operations, cyber operations, doctrine, cyber intelligence, and multilateral data and information functions. The diversity of functional backgrounds was intended to capture different perspectives concerning technology, operational strategy, naval posture, information systems, and maritime security threats.

The seven experts were selected based on their professional responsibilities, experience, and knowledge relevant to the development and implementation of Indonesian maritime defense capabilities. Their judgments were used primarily to identify the relevant Smart Defense dimensions and variables and subsequently to determine their relative importance. Thus, the expert panel functioned as a structured source of domain knowledge rather than as a conventional statistical sample.

The combination of expert judgment and documentary information was considered appropriate because several dimensions of maritime defense capability, particularly strategic posture, threat perception, and future technological requirements, cannot be adequately represented using historical quantitative data alone.

Delphi Method

The Delphi method was applied to identify and refine the principal dimensions and criteria considered relevant to Smart Defense. The method was selected because the research involves complex defense issues requiring informed judgment from experts with different areas of professional specialization. The Delphi process provides a structured mechanism for obtaining expert consensus and reducing an initially broad set of potential variables to the most relevant dimensions.

In the initial stage, the study considered seven potential criteria associated with Smart Defense. The experts evaluated the importance of each criterion using a 1–9 importance scale. The scores obtained from the seven experts were aggregated and converted into mean values. A criterion was retained when its mean expert score exceeded the predetermined threshold of 7.00.

The Delphi assessment resulted in four principal dimensions being retained:

1. **Technology (K3)** – mean score **8.57**;
2. **Operational Strategy (K1)** – mean score **8.43**;
3. **Indonesian Navy Posture (K2)** – mean score **8.00**; and
4. **Threat Perception (K4)** – mean score **7.86**.

The remaining three criteria did not meet the retention threshold. Their mean scores were 5.14, 3.71, and 3.86, respectively, and they were therefore excluded from the final model.

The Delphi results indicate a high level of expert agreement concerning the relevance of the four retained dimensions. More importantly, the results support the multidimensional conceptualization of Smart Defense developed in Section 2.4. Smart Defense is therefore operationalized in the subsequent analysis through Technology, Operational Strategy, Indonesian Navy Posture, and Threat Perception.

Fuzzy Weighting

Following the Delphi process, Fuzzy Weighting was employed to determine the relative importance of the retained Smart Defense dimensions and their associated criteria. The use of fuzzy weighting was intended to address the uncertainty and ambiguity inherent in linguistic expert judgments. Rather than treating expert assessments as precise deterministic values, the approach translates linguistic evaluations into numerical representations that can subsequently be aggregated and normalized.

The procedure involved assigning numerical values to the linguistic importance judgments provided by the experts, followed by aggregation, defuzzification, and normalization. The resulting normalized weights represent the relative contribution or priority of each principal dimension within the Smart Defense framework. The resulting weights for the four principal dimensions are presented in Table 1.

Table 1. Smart Defense Dimension Weights

Smart Defense Dimension	Weight
Technology	0.27
Indonesian Navy Posture	0.26
Threat Perception	0.24
Operational Strategy	0.23
Total	1.00

Table 1 shows that Technology received the highest overall weight of **0.27**, followed by Indonesian Navy Posture (**0.26**), Threat Perception (**0.24**), and Operational Strategy (**0.23**). The relatively close distribution of the four weights indicates that Smart Defense is not dominated by a single dimension. Instead, the overall capability depends on the balanced contribution of technological capability, operational effectiveness, naval posture, and awareness of the threat environment.

At the criterion level, several variables emerged as particularly important. Within the Technology dimension, the key variables included Integrated System, Monitoring, Cyber, Big Data/IoT/AI/Machine Learning, and Autonomous Capability. Within Operational Strategy, important criteria included Anti-Submarine Warfare, Coastal Defense, Sea Control, Command and Control, and Mobile Surveillance. Within the Indonesian Navy Posture dimension, Integrated Fleet Weapon System (SSAT) received the highest criterion weight. These criterion-level priorities were subsequently incorporated into the System Dynamics model.

System Dynamics Model Development

The weighted variables were subsequently incorporated into a System Dynamics model to represent the interactions among the four principal dimensions of Smart Defense. System Dynamics was selected because the research problem involves interdependent variables, feedback relationships, accumulation, and changes over time. The approach enables the model to represent Smart Defense as a dynamic system rather than as a static aggregate index.

The conceptual structure was first represented through causal relationships among the principal variables. These relationships were then translated into stock-and-flow structures consisting of stocks, flows, and auxiliary variables. The model was developed using Stella 9.1.3.

At the aggregate level, the Smart Defense index was represented using the following weighted formulation:

$$[SD(t)=0.27T(t)+0.23O(t)+0.26P(t)+0.24A(t)]$$

where:

- **SD(t)** = Smart Defense capability at time t ;
- **T(t)** = Technology dimension;
- **O(t)** = Operational Strategy dimension;
- **A(t)** = Threat Perception dimension, operationalized as the capability to identify, assess, anticipate, and respond to changing maritime threats.
- **A(t)** = Threat Perception dimension.

The weighting coefficients correspond to the results obtained through the Fuzzy Weighting process. The formulation provides the aggregate structure of the Smart Defense index, while the System Dynamics implementation represents the internal relationships among the variables within each dimension.

Within the Technology dimension, the model incorporates variables such as Integrated System and Big Data. Within Operational Strategy, the model includes Logistics, Command and Control, Sea Control, and related operational capabilities. Within Indonesian Navy Posture, the model incorporates SSAT and deployment-related variables. The Threat Perception dimension incorporates maritime cyber-security threats and changing maritime security conditions, with higher scores representing stronger threat awareness and response capability.

The model therefore does not merely calculate a weighted index at a single point in time. Instead, it allows changes in the component variables to influence the overall Smart Defense capability through the modeled relationships and dynamic interactions.

Model Verification and Validation

Model verification and validation were conducted to determine whether the System Dynamics model was logically consistent, structurally acceptable, and sufficiently representative for the intended analytical purpose.

First, model verification was conducted by examining the model logic, equations, relationships, and unit consistency in Stella. The model and its four principal sub-models were checked to ensure that the equations were formulated correctly and

that the model could operate throughout the five-year projection interval without formulation or unit errors.

Second, structural validation was conducted through expert assessment of the causal-loop structure and the adequacy of the variables incorporated into the model. All seven experts accepted the proposed model structure, indicating that the relationships among the principal dimensions and variables were considered sufficiently representative of the Smart Defense system.

Third, quantitative validation was conducted by comparing the simulated and actual values. The model generated a simulated value of 7.43 for 2023, compared with an actual value of 7.12. The reported mean error was 0.04353, which was below the 0.10 validation threshold used in the study. Based on this criterion, the model was considered quantitatively valid for the analysis.

The combination of structural and quantitative validation provides greater confidence that the model can be used to examine the behavior of Smart Defense and to evaluate alternative policy scenarios. Nevertheless, the model should be interpreted as a policy-oriented analytical representation rather than as a deterministic prediction of future defense conditions.

Sensitivity Analysis and Policy Scenarios

Sensitivity analysis was conducted to identify the variables that exerted the strongest influence on the Smart Defense capability. The analysis focused on determining which variables within each principal dimension generated the greatest change in the overall system when their values were modified.

Four key variables were identified through the sensitivity analysis:

1. **Integrated System** as the key variable within the Technology dimension;
2. **Logistics** as the key variable within the Operational Strategy dimension;
3. **Integrated Fleet Weapon System (SSAT)** as the key variable within the Indonesian Navy Posture dimension; and
4. **Maritime Cyber Security Threat** as the key variable within the Threat Perception dimension.

These variables were subsequently used as the basis for policy scenario development. Four alternative scenarios were constructed for the 2023–2028 projection interval. Each scenario examined the potential effect of strengthening or changing one of the key variables while maintaining the remaining model structure.

The scenarios were designed as follows (Table 2).

Table 2. Scenarios and Policy Interventions

Scenario	Policy Intervention
S0 – Business as Usual	Baseline condition without additional intervention
S1 – Technological Integration	Strengthening Integrated System and related technological integration
S2 – Operational Logistics	Strengthening logistics capability within Operational Strategy
S3 – SSAT Strengthening	Strengthening the Integrated Fleet Weapon System

Scenario	Policy Intervention
S4 – Maritime Cyber Threat	Increasing perceived maritime cyber-security threat without proportional capability strengthening

The scenario analysis enables the study to move beyond identifying important variables toward evaluating the potential consequences of alternative policy interventions. The results are subsequently presented in Section 4, where the Delphi results, Fuzzy Weighting results, baseline model behavior, sensitivity analysis, and policy scenarios are analyzed.

RESULTS

Delphi Results

The Delphi assessment was conducted to identify the principal dimensions that should be retained in the Smart Defense model. The initial assessment considered seven potential criteria. Based on the expert evaluation using a 1–9 importance scale, four dimensions achieved mean scores above the predetermined threshold of 7.00 and were therefore retained in the final model.

As presented in Table 3, Technology obtained the highest mean score of 8.57, followed by Operational Strategy with a mean score of 8.43, Indonesian Navy Posture with 8.00, and Threat Perception with 7.86. The remaining three criteria obtained mean scores of 5.14, 3.71, and 3.86 and were excluded from the subsequent analysis.

Table 3. Delphi Assessment of Smart Defense Dimensions

Criterion	Expert Score	Mean Score	Decision
Technology (K3)	60	8.57	Retained
Operational Strategy (K1)	59	8.43	Retained
Indonesian Navy Posture (K2)	56	8.00	Retained
Threat Perception (K4)	55	7.86	Retained
Criterion K5	36	5.14	Excluded
Criterion K6	26	3.71	Excluded
Criterion K7	27	3.86	Excluded
Retention threshold	—	>7.00	—

The Delphi results establish that Smart Defense in the Indonesian maritime defense context is multidimensional. Although Technology received the highest expert assessment, the relatively high scores obtained by Operational Strategy, Indonesian Navy Posture, and Threat Perception indicate that Smart Defense cannot be represented adequately by technological capability alone. The four retained dimensions were therefore used as the principal components of the subsequent Fuzzy Weighting and System Dynamics analyses.

Fuzzy Weighting Results

Following the Delphi assessment, Fuzzy Weighting was applied to determine the relative importance of the four retained dimensions. The results indicate that Technology

received the highest weight at 0.27, followed by Indonesian Navy Posture at 0.26, Threat Perception at 0.24, and Operational Strategy at 0.23.

Table 4. Fuzzy Weights of the Principal Smart Defense Dimensions

Rank	Dimension	Weight	Percentage
1	Technology	0.27	27%
2	Indonesian Navy Posture	0.26	26%
3	Threat Perception	0.24	24%
4	Operational Strategy	0.23	23%
	Total	1.00	100%

As presented in Table 4, the difference between the highest and lowest weights is only 0.04. This indicates that the four dimensions have relatively balanced contributions to the Smart Defense system. Technology has the highest priority, but its weight is not sufficiently dominant to suggest that Smart Defense can be achieved through technology development alone.

At the criterion level, the results identified several variables with relatively strong contributions within their respective dimensions. Within the Technology dimension, Integrated System was identified as an important variable, together with Monitoring, Cyber, Big Data/IoT/AI/Machine Learning, and Autonomous Capability. Within Operational Strategy, important variables included Logistics, Command and Control, Sea Control, Coastal Defense, and Mobile Surveillance. Within the Indonesian Navy Posture dimension, Integrated Fleet Weapon System (SSAT) emerged as the most important criterion. Maritime Cyber Security Threat represented the key variable within the Threat Perception dimension. The resulting weights were subsequently incorporated into the System Dynamics model as the relative contribution coefficients of the four principal dimensions.

System Dynamics Model and Baseline Results

The System Dynamics model was developed to represent the dynamic interactions among Technology, Operational Strategy, Indonesian Navy Posture, and Threat Perception in determining Smart Defense capability. The model was structured based on the causal relationships identified through the literature review and expert assessment. The four dimensions were not treated as independent components; rather, they were connected through reinforcing and balancing relationships that represent the dynamic behavior of the maritime defense system.

Figure 2 presents the Causal Loop Diagram (CLD) developed for the Smart Defense system.

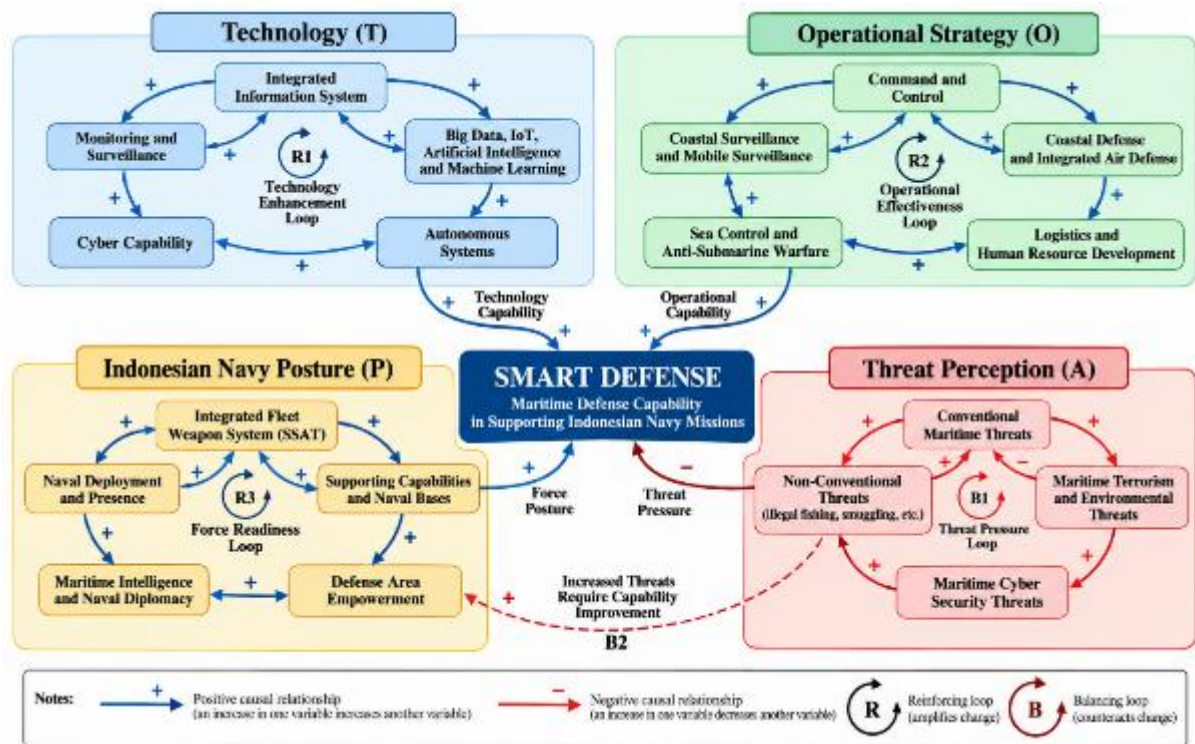


Figure 2. Causal Loop Diagram of Smart Defense for Indonesia's Archipelagic Maritime Defense Strategy

The CLD illustrates several important feedback mechanisms. Within the Technology subsystem, improvements in integrated information systems, monitoring and surveillance, cyber capability, Big Data, Artificial Intelligence, Machine Learning, and autonomous systems reinforce technological capability. This relationship is represented by the Technology Enhancement Loop (R1). Greater technological integration improves the availability and quality of information, which subsequently supports more effective maritime surveillance and operational decision-making.

Within the Operational Strategy subsystem, improvements in command and control, surveillance, coastal defense, sea control, anti-submarine warfare, logistics, and human-resource development reinforce operational effectiveness. This relationship is represented by the Operational Effectiveness Loop (R2). Improvements in operational capability contribute positively to Smart Defense and provide the operational foundation for sustained maritime missions.

The Indonesian Navy Posture subsystem is represented through the interaction among the Integrated Fleet Weapon System (SSAT), naval deployment and presence, supporting capabilities, naval bases, maritime intelligence, naval diplomacy, and defense-area empowerment. These relationships form the Force Readiness Loop (R3). Strengthening the naval posture increases the ability to deploy and sustain maritime forces, which in turn contributes positively to Smart Defense.

The Threat Perception subsystem introduces both reinforcing and balancing effects into the overall system. Increasing conventional, non-conventional, maritime terrorism, environmental, and cyber-security threats increases pressure on the defense

system. This relationship is represented by the Threat Pressure Loop (B1). When threat levels increase without corresponding improvements in defense capability, the overall Smart Defense capability may decline. Conversely, increased threat awareness can create pressure for capability improvement, generating a balancing response within the system.

The interaction among these subsystems demonstrates that Smart Defense is an emergent capability generated by the combined effects of technology, operational effectiveness, naval posture, and threat conditions. Improvements in one dimension can strengthen other dimensions, while increasing threats can generate additional capability requirements. This dynamic structure provides the basis for translating the causal relationships into the stock-and-flow model used for simulation.

Following the development of the causal structure, the model was simulated over the 2023–2028 projection interval to establish the baseline trajectory of Smart Defense capability. The baseline simulation indicates that the overall Smart Defense capability index increases from 8.68 (86.8%) in 2023 to 8.88 (88.8%) in 2028. Both values remain within the Capable/Excellent classification used in the study.

Table 5. Baseline Smart Defense Capability, 2023–2028

Indicator	2023	2028	Interpretation
Overall Smart Defense	8.68 / 86.8%	8.88 / 88.8%	Capable/Excellent
Technology	—	8.81	High capability
Operational Strategy	—	7.90	Moderate–high capability
Indonesian Navy Posture	—	6.29	Priority for strengthening
Threat Perception	—	8.11	High threat-awareness and response capability

As presented in Table 5, the baseline results indicate a positive development in the aggregate Smart Defense capability during the simulation period. However, the component results reveal an uneven distribution of capability across the four dimensions. Technology achieves the highest 2028 value at 8.81, followed by Threat Perception at 8.11 and Operational Strategy at 7.90. Indonesian Navy Posture records the lowest value at 6.29, indicating a comparatively weaker component within the overall system.

This result is important because a relatively high aggregate Smart Defense index does not necessarily imply that all capability dimensions are equally strong. The comparatively lower value of Indonesian Navy Posture suggests that force structure, SSAT, deployment, supporting capabilities, and related naval posture variables require particular attention in subsequent policy analysis.

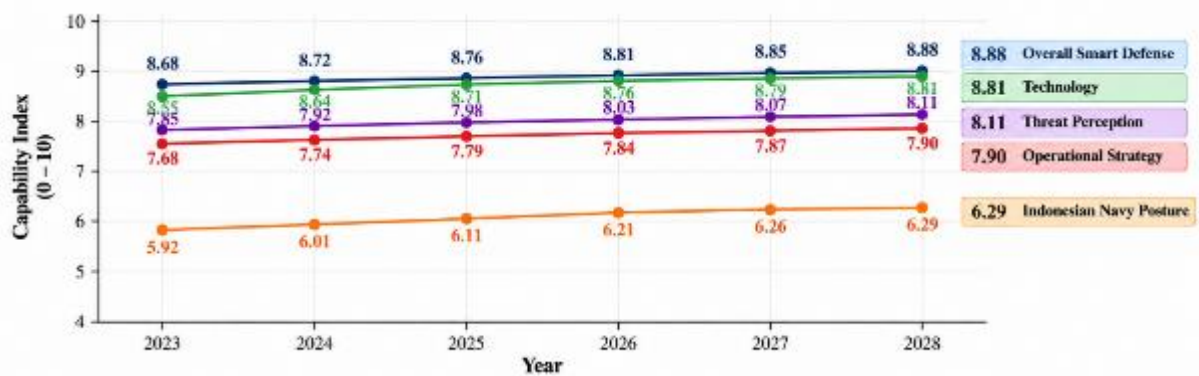


Figure 3. The baseline development of the Smart Defense capability index

Figure 3 presents the baseline development of the Smart Defense capability index and its four component dimensions during the 2023–2028 projection interval. The overall Smart Defense index increases from 8.68 in 2023 to 8.88 in 2028, indicating a positive but moderate improvement in the overall capability. Throughout the projection interval, the overall index remains within the Capable/Excellent category used in the study.

Among the four component dimensions, Technology consistently records the highest value, increasing from 8.55 in 2023 to 8.81 in 2028. Threat Perception also demonstrates a steady increase, from 7.85 to 8.11, while Operational Strategy increases from 7.68 to 7.90. These three dimensions demonstrate relatively high and stable performance throughout the projection interval.

In contrast, Indonesian Navy Posture remains the lowest-performing dimension, although it also shows gradual improvement from 5.92 in 2023 to 6.29 in 2028. The difference between this dimension and the other three components indicates a structural capability gap within the overall Smart Defense system. Thus, although the aggregate Smart Defense index remains in the Capable/Excellent category, the Indonesian Navy Posture dimension represents a priority area for further capability strengthening.

The baseline trajectory also demonstrates that improvements in the overall Smart Defense index are relatively gradual under the existing system conditions. The increase from 8.68 to 8.88 over five years suggests that maintaining the current development pattern produces only a modest improvement. This finding provides the basis for the subsequent sensitivity analysis and policy scenario analysis, which examine whether targeted interventions in specific variables can generate greater improvements in Smart Defense capability.

Sensitivity Analysis Results

Sensitivity analysis was conducted to identify the variables that exerted the strongest influence on the Smart Defense system. The analysis identified one key variable within each of the four principal dimensions.

The Integrated System variable was identified as the most influential variable within the Technology dimension. This finding indicates that technological capability is strongly dependent on the degree to which information, surveillance, communication, and other technological resources are integrated rather than developed independently.

Within the Operational Strategy dimension, Logistics emerged as the key variable. Logistics provides the operational support necessary for sustained maritime operations, deployment, command and control, and sea-control activities.

Within the Indonesian Navy Posture dimension, Integrated Fleet Weapon System (SSAT) was identified as the most influential variable. This result indicates the importance of an integrated naval force structure in determining the effectiveness of maritime defense capability.

Finally, Maritime Cyber Security Threat emerged as the key variable associated with Threat Perception. The sensitivity result indicates that changes in the maritime cyber-security environment can substantially influence the overall Smart Defense system, particularly when changes in threat conditions are not accompanied by proportional improvements in defense capability.

Table 6. Key Variables Identified Through Sensitivity Analysis

Principal Dimension	Key Variable	Model Significance
Technology	Integrated System	Key technological integration variable
Operational Strategy	Logistics	Key operational-support variable
Indonesian Navy Posture	SSAT	Key naval capability variable
Threat Perception	Maritime Cyber Security Threat	Key changing-threat variable

As presented in Table 6, the sensitivity results were subsequently used to formulate four policy scenarios. The selection of these variables provides a direct methodological connection between sensitivity analysis and scenario-based policy evaluation.

Four policy scenarios were simulated to examine how changes in the key variables identified through sensitivity analysis could affect Smart Defense capability.

Four policy scenarios were simulated to examine how changes in the key variables identified through sensitivity analysis could affect Smart Defense capability.

Table 7. Policy Scenario Results

Scenario Policy Focus		Smart Defense Score (2023 → 2028)	Change
S0	Business as Usual	Baseline	—
S1	Strengthening Integrated System and Big Data	8.16 → 8.33	+2.08%
S2	Strengthening Logistics	7.44 → 7.46	+0.27%
S3	Strengthening SSAT by 30%	7.42 → 7.73	+4.17%

Scenario Policy Focus		Smart Defense Score (2023 → 2028)	Change
S4	Increasing maritime cyber-security threat pressure	7.18 → 7.06	-1.67%

As presented in Table 7, the results demonstrate that Scenario 3 (SSAT Strengthening) generates the largest improvement in Smart Defense capability. Increasing SSAT by 30% produces a 4.17% improvement, making it the strongest positive intervention among the scenarios examined.

Scenario 1, which focuses on technological integration through Integrated System and Big Data, produces the second-largest improvement, with a 2.08% increase. This result demonstrates the positive contribution of integrated technological capability to Smart Defense performance.

Scenario 2, which strengthens Logistics, produces a comparatively smaller direct improvement of 0.27%. Nevertheless, the result indicates a positive contribution of logistics to the overall system.

In contrast, Scenario 4 produces a negative result. Increasing the Maritime Cyber Security Threat variable from 7.18 to 7.06 results in a 1.67% reduction in the Smart Defense index. This finding indicates that increasing threat conditions without a corresponding increase in defense capability may weaken overall Smart Defense performance.

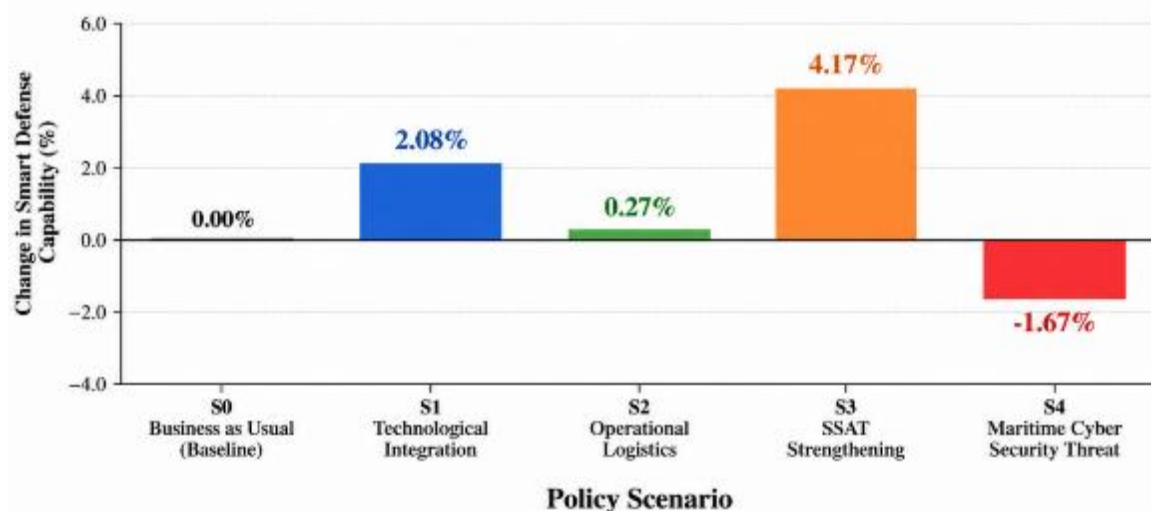


Figure 4. Comparison of Policy Scenario Effects on Smart Defense

Figure 4 compares the relative effects of the four policy interventions on Smart Defense capability against the Business-as-Usual (S0) baseline. The results show clear differences in the effectiveness of the simulated interventions. Among the positive scenarios, S3 – SSAT Strengthening produces the largest improvement, with a 4.17% increase in Smart Defense capability. This result indicates that strengthening the

Integrated Fleet Weapon System (SSAT) has the strongest direct effect among the policy interventions examined.

The second-largest improvement is generated by S1 – Technological Integration, which increases the Smart Defense capability by 2.08%. This scenario emphasizes the strengthening of Integrated System and Big Data, indicating that improvements in technological integration can contribute substantially to overall Smart Defense capability. However, its effect remains lower than that of SSAT strengthening.

S2 – Operational Logistics produces a relatively modest positive effect of 0.27%. Although the magnitude is substantially smaller than those of S1 and S3, the positive result indicates that strengthening logistics contributes to the sustainability of maritime defense operations. The relatively limited direct effect in the simulation does not necessarily imply that logistics is strategically unimportant, because logistics functions as an enabling component supporting other operational capabilities.

In contrast, S4 – Maritime Cyber Security Threat produces a negative effect of -1.67%. This scenario represents an increase in maritime cyber-security threat pressure without a proportional strengthening of supporting defense capability. The negative result indicates that increasing threat pressure can reduce overall Smart Defense performance when capability development does not keep pace with the changing threat environment.

Overall, Figure 4 demonstrates that capability-oriented interventions generate positive effects, whereas an increase in threat pressure without corresponding capability reinforcement produces a negative outcome. The results therefore suggest that Smart Defense improvement should prioritize strengthening deployable naval capability, technological integration, and operational support while simultaneously developing adequate capabilities to anticipate and respond to emerging maritime cyber-security threats. These findings provide an important basis for the strategic interpretation and policy implications discussed in Section 5.

Summary of Key Results

The results can be summarized into five principal findings. First, the Delphi process reduced the initial set of seven potential criteria to four principal Smart Defense dimensions: Technology, Operational Strategy, Indonesian Navy Posture, and Threat Perception. Second, Fuzzy Weighting produced relatively balanced dimension weights, with Technology receiving the highest weight of 0.27, followed by Indonesian Navy Posture (0.26), Threat Perception (0.24), and Operational Strategy (0.23).

Third, the baseline System Dynamics model projects an increase in overall Smart Defense capability from 86.8% in 2023 to 88.8% in 2028, remaining within the Capable/Excellent classification. Fourth, the component results indicate that Indonesian Navy Posture is the comparatively weaker dimension, with a 2028 value of 6.29, despite the relatively high overall Smart Defense score. Fifth, the policy scenario analysis demonstrates that SSAT strengthening produces the strongest positive effect (+4.17%), followed by technological integration (+2.08%) and logistics strengthening (+0.27%). Conversely, increasing maritime cyber-security threats without proportional capability reinforcement produces a negative effect of -1.67%.

Overall, the results demonstrate that Smart Defense performance is determined by the interaction of multiple capability dimensions rather than by a single technological or force-development variable. These empirical findings provide the basis for the discussion of theoretical implications, strategic interpretation, and policy implications in the next section.

DISCUSSION

Smart Defense as an Integrated Capability System

The findings demonstrate that Smart Defense should be understood as an integrated capability system rather than as a technology acquisition program. The Delphi assessment identified four principal dimensions—Technology, Operational Strategy, Indonesian Navy Posture, and Threat Perception—while the Fuzzy Weighting results showed relatively balanced weights across these dimensions. Although Technology received the highest weight (0.27), its difference from Indonesian Navy Posture (0.26), Threat Perception (0.24), and Operational Strategy (0.23) was relatively small. This indicates that Smart Defense capability is dependent on the interaction and alignment of multiple dimensions rather than on technological superiority alone.

This finding is consistent with contemporary maritime capability research, which emphasizes the importance of integrating organizational capacity, operational requirements, technology, and resilience rather than relying on isolated capabilities (Bueger et al., 2020; Canepa et al., 2021; Taddeo et al., 2021). In the Indonesian maritime context, this integrated perspective is particularly important because technological systems must operate within an organizational and operational structure capable of converting information and technological advantages into effective maritime action.

The System Dynamics structure further reinforces this interpretation. Technology, operational strategy, naval posture, and threat perception are connected through feedback relationships rather than functioning as independent variables. Consequently, improvements in one dimension can generate effects in other dimensions, while weaknesses in one component can constrain the performance of the overall system. Smart Defense should therefore be viewed as an emergent capability produced by the interaction among technological, organizational, operational, and threat-related factors.

Technology Integration and the Role of Interoperability

Technology received the highest weight in the Fuzzy Weighting analysis, with a value of 0.27, and remained the highest-performing component in the baseline simulation. This finding confirms the growing importance of integrated technological capability in contemporary maritime defense. However, the results should not be interpreted as indicating that the acquisition of advanced technology alone will automatically generate superior defense capability.

The sensitivity analysis identified **Integrated System** as the key variable within the Technology dimension. This finding emphasizes the importance of interoperability and integration among information systems, monitoring and surveillance, cyber capability, Big Data, Internet of Things, Artificial Intelligence, Machine Learning, and autonomous systems. The technological value of these capabilities depends not only on

their individual performance but also on their ability to exchange information and support coordinated decision-making.

The finding is consistent with recent research emphasizing the importance of integrated information systems, digitalization, interoperability, and cybersecurity in maritime operations (Ben Farah et al., 2022; Bolbot et al., 2022; Kuhn et al., 2021). In the present study, however, technology is positioned within a broader system that includes operational strategy, naval posture, and threat perception. Thus, the contribution of technology is strengthened when it is connected to operational requirements and force capabilities.

The positive result of Scenario 1, which increased Smart Defense capability by 2.08%, provides further support for this interpretation. Technological integration produces a meaningful improvement, but the effect remains smaller than the effect of SSAT strengthening. This indicates that technology should function as an enabler of operational and force capabilities rather than as a substitute for them.

Naval Posture as a Critical Capability Gap

One of the most important findings of the study is the comparatively lower performance of the Indonesian Navy Posture dimension. Although Indonesian Navy Posture received a relatively high Fuzzy Weighting value of 0.26, its 2028 baseline value was only 6.29, substantially below Technology (8.81), Threat Perception (8.11), and Operational Strategy (7.90). This difference reveals an important structural capability gap that is not visible from the aggregate Smart Defense index alone.

The result becomes particularly significant when combined with the policy scenario analysis. Scenario 3, which strengthens SSAT by 30%, generated the largest improvement in Smart Defense capability at 4.17%. This result indicates that force posture remains a critical determinant of maritime defense effectiveness even within an increasingly technology-intensive defense environment.

The finding is consistent with the contemporary Indonesian maritime perspective, in which strategic geography, maritime presence, and national maritime interests remain central to defense planning (Pertiwi, 2020). In the contemporary context, however, naval posture extends beyond the number of platforms. It encompasses the integration of SSAT, deployment patterns, supporting capabilities, naval bases, maritime intelligence, defense-area empowerment, and operational readiness.

The result also reinforces the importance of integrating force modernization with deployment and operational requirements. A technologically advanced defense system cannot generate its full strategic value if the corresponding naval forces are insufficiently integrated, deployed, supported, or maintained. Therefore, the comparatively strong effect of SSAT strengthening suggests that Smart Defense should retain a strong physical and operational capability foundation.

Operational Strategy and the Enabling Role of Logistics

Operational Strategy received the lowest of the four principal Fuzzy Weighting values, at 0.23. Nevertheless, this result should not be interpreted as indicating that operational strategy is of secondary strategic importance. Rather, its relatively lower

weight reflects its position within an integrated capability system in which operational effectiveness depends on the availability of technology, force posture, logistics, and supporting capabilities.

The sensitivity analysis identified Logistics as the key variable within the Operational Strategy dimension. Logistics provides the supporting foundation for sustained maritime operations, deployment, command and control, sea control, surveillance, and other operational activities. Without adequate logistics, improvements in platforms and technology may not be translated into sustained operational effectiveness.

Scenario 2 produced an improvement of **0.27%**, which was substantially smaller than the effects of SSAT strengthening and technological integration. This relatively modest direct effect should not be interpreted as evidence that logistics is unimportant. Rather, logistics functions as an enabling mechanism whose contribution is distributed across other parts of the defense system. Its effects may therefore be less visible as a direct change in the aggregate index while remaining essential for maintaining operational continuity.

This finding is particularly relevant to the System Dynamics perspective because enabling variables may influence system performance indirectly through multiple causal pathways. Consequently, policy prioritization should not rely exclusively on the magnitude of a variable's direct scenario effect but should also consider its role in sustaining other components of the system.

Threat Perception and Maritime Cyber-Security Resilience

The Threat Perception dimension received a Fuzzy Weighting value of 0.24 and reached a relatively high baseline value of 8.11 in 2028. In the model, this score represents the capability to recognize, assess, and respond to the maritime security environment; it should therefore be distinguished from the intensity of the external threat itself. The scenario analysis demonstrates that threat awareness and defense capability are not equivalent.

Scenario 4, which increases Maritime Cyber Security Threat pressure without proportional capability strengthening, produces a 1.67% decline in Smart Defense capability. This negative result is important because it demonstrates the balancing relationship represented in the System Dynamics model: increasing threat pressure can reduce system performance when capability development does not keep pace with the threat environment.

The result highlights the importance of treating maritime cyber security as an operational and strategic defense capability rather than solely as an information-technology issue. Recent studies identify growing cyber vulnerabilities in maritime systems and emphasize the need for detection, protection, response, recovery, risk assessment, and organizational preparedness (Afenyo & Caesar, 2023; Drazovich et al., 2021; Erstad et al., 2021; Kanwal et al., 2022; Karamperidis et al., 2021; Kuhn et al., 2021; Larsen & Lund, 2021; Meland et al., 2021; Park et al., 2023; Schinas & Metzger, 2023). In this sense, threat perception should serve not only as an indicator of environmental pressure but also as a trigger for capability adaptation.

This finding also reinforces the dynamic character of Smart Defense. A defense system that performs adequately under one threat condition may become less effective when threat intensity or characteristics change. Consequently, maritime defense planning should continuously adjust capability development in response to changes in the security environment.

Theoretical Contribution of the System Dynamics Approach

The principal theoretical contribution of this study lies in connecting the Smart Defense concept with a dynamic capability-system perspective. Recent maritime research has largely examined technological integration, cybersecurity, autonomous systems, and maritime operational resilience as interconnected but often separately analyzed domains (Akdağ et al., 2022; Bolbot et al., 2022; Tai et al., 2021). The present study extends this perspective by integrating expert-based variable identification, quantitative weighting, and dynamic simulation into a single analytical framework.

The System Dynamics approach contributes by demonstrating that Smart Defense performance cannot be adequately understood through static relationships alone. Technology, operational strategy, naval posture, and threat perception interact through reinforcing and balancing mechanisms. Changes in one component can therefore influence the behavior of the broader system over time.

The study also contributes methodologically by linking Delphi → Fuzzy Weighting → System Dynamics. Delphi provides expert-based identification of relevant dimensions, Fuzzy Weighting quantifies their relative importance, and System Dynamics translates these weighted relationships into a dynamic representation. This sequential integration provides a structured pathway for converting expert knowledge into a policy-oriented analytical model.

The resulting framework is particularly relevant for complex defense environments in which historical data may be limited, several variables are difficult to measure directly, and future capability development depends on strategic assumptions and expert knowledge. The study therefore demonstrates how qualitative defense expertise can be integrated with quantitative modeling without reducing the problem to a purely statistical relationship.

Strategic Implications for Indonesian Maritime Defense

The findings have several strategic implications for the development of Smart Defense within Indonesia's Archipelagic Maritime Defense Strategy. First, capability development should prioritize integration rather than isolated acquisition. Investments in Big Data, IoT, Artificial Intelligence, Machine Learning, autonomous systems, surveillance, and cyber capability should be connected through interoperable information and command architectures (Akdağ et al., 2022; Liu et al., 2022; Taddeo et al., 2021; Vagale et al., 2021; Zhang et al., 2021; Ziajka-Poznańska & Montewka, 2021).

Second, the results indicate that SSAT and naval force posture require particular attention. The comparatively low baseline value of Indonesian Navy Posture and the strongest scenario effect generated by SSAT strengthening suggest that force modernization should be closely connected with deployment, intelligence, security, support, readiness, and operational requirements (Bueger et al., 2020; Pertiwi, 2020).

Third, maritime cyber-security resilience should be treated as a core defense capability. The negative result of the threat scenario demonstrates that increasing cyber threats without proportional capability development can reduce overall Smart Defense performance. Cyber-security planning should therefore be integrated with operational planning and broader maritime defense capability development (Afenyo & Caesar, 2023; Erstad et al., 2021; Karamperidis et al., 2021; Meland et al., 2021; Schinas & Metzger, 2023).

Fourth, logistics and command-and-control capabilities should continue to be strengthened. Although the direct effect of the logistics scenario was relatively modest, logistics provides the operational foundation required for sustained maritime presence and sea-control activities (Canepa et al., 2021).

Finally, the System Dynamics model should be regarded as a decision-support instrument rather than a one-time forecasting tool. Because technology, force structures, organizational arrangements, budgets, and threat conditions can change, the model can be periodically updated with new expert assessments and operational data. This would allow the model to support continuing strategic capability planning (Tai et al., 2021; Drazovich et al., 2021).

Overall Discussion

Taken together, the findings demonstrate that the most effective approach to Smart Defense is not to maximize a single capability dimension but to develop a balanced and integrated capability architecture. Technology provides an important foundation, but its value depends on operational strategy, naval posture, and the ability to respond to changing threats.

The strongest scenario effect generated by SSAT strengthening, followed by technological integration and logistics, demonstrates that Indonesia's maritime defense capability requires both high-technology integration and credible deployable force capability. At the same time, the negative effect associated with increasing maritime cyber-security threats demonstrates that capability development must remain adaptive to changes in the threat environment.

Therefore, the central implication of this study is that Smart Defense should be implemented as an integrated capability-development strategy combining technology, operations, naval force posture, logistics, and cyber-security resilience. Such an approach is more consistent with the systemic and dynamic characteristics of Indonesia's maritime defense environment than a strategy based solely on technology acquisition or force expansion.

CONCLUSION

Conclusion

This study developed a System Dynamics model to assess Smart Defense within Indonesia's Archipelagic Maritime Defense Strategy (SPLN) by integrating expert-based Delphi assessment, Fuzzy Weighting, and System Dynamics modeling. The study demonstrates that Smart Defense should be understood as an integrated maritime defense capability involving technological, operational, organizational, and threat-related dimensions rather than as a technology acquisition program alone.

The Delphi assessment identified four principal dimensions of Smart Defense: Technology, Operational Strategy, Indonesian Navy Posture, and Threat Perception. Fuzzy Weighting subsequently assigned relative weights of 0.27, 0.23, 0.26, and 0.24, respectively. Although Technology received the highest weight, the relatively small differences among the four dimensions indicate that Smart Defense depends on the balanced interaction of technological capability, operational effectiveness, naval force posture, and awareness of the maritime security environment.

The baseline System Dynamics simulation indicates that the overall Smart Defense capability increases from 86.8% in 2023 to 88.8% in 2028, remaining within the Capable/Excellent category. However, the component-level results reveal an important capability gap. By 2028, Technology reaches 8.81, Threat Perception reaches 8.11, and Operational Strategy reaches 7.90, whereas Indonesian Navy Posture reaches only 6.29. This finding indicates that a relatively high aggregate capability score may coexist with weaknesses in specific dimensions.

The sensitivity and policy scenario analyses provide further evidence concerning capability priorities. Integrated System, Logistics, Integrated Fleet Weapon System (SSAT), and Maritime Cyber Security Threat were identified as key variables within their respective dimensions. Among the policy scenarios, strengthening SSAT by 30% generated the largest improvement in Smart Defense capability (+4.17%), followed by technological integration through Integrated System and Big Data (+2.08%) and operational logistics (+0.27%). Conversely, increasing Maritime Cyber Security Threat without proportional capability reinforcement reduced the Smart Defense index by 1.67%.

The principal conclusion is therefore that Smart Defense should be implemented as an integrated capability-development strategy. Technological modernization needs to be accompanied by effective operational strategy, adequate naval force posture, sustainable logistics, and strengthened maritime cyber-security resilience. In particular, the strong effect of SSAT strengthening indicates that technological advancement should be complemented by credible and deployable naval capabilities.

From a methodological perspective, the integration of Delphi, Fuzzy Weighting, and System Dynamics provides a structured approach for transforming expert knowledge into a quantitative and dynamic decision-support model. The model enables defense planners to identify capability priorities, examine interactions among critical variables, and assess alternative policy interventions over time. Thus, the study contributes not only to the understanding of Smart Defense in the Indonesian maritime context but also to the development of a systematic approach for supporting maritime defense capability planning.

Limitations and Future Research

This study has several limitations. First, the model is based on a seven-member expert panel, and therefore the results primarily represent structured expert judgment rather than a large statistical sample. Second, several model parameters and relationships are derived from expert assessments and strategic assumptions, while maritime defense conditions, organizational structures, technologies, budgets, and

threat characteristics may change over time. Third, the simulation covers a five-year period from 2023 to 2028 and should therefore be interpreted as a policy-oriented projection rather than a deterministic forecast.

Future research should expand the expert panel and incorporate more extensive longitudinal and operational data to improve model robustness. Further studies may also compare alternative weighting approaches, examine interactions among maritime, air, land, cyber, and civilian components of national defense, and test the model under different strategic and technological conditions. Comparative research involving Smart Defense frameworks in other maritime countries would also provide opportunities to assess the transferability and broader applicability of the proposed model.

Authors' Contributions

J.P. Conceptualization, research design, data collection, expert assessment, methodology, System Dynamics modeling, data analysis, and preparation of the original manuscript. **O.S.S.** Conceptualization, methodology, interpretation of results, critical review, and revision of the manuscript. **S.W.H.** Data interpretation, validation, analysis of maritime defense strategy, and critical review of the manuscript. **E.K.** Expert assessment, interpretation of Indonesian Navy operational and defense aspects, critical review, and revision of the manuscript. All authors contributed to the development of the research, reviewed the manuscript critically, approved the final version, and agreed to be accountable for all aspects of the work.

Declaration of Conflict of Interest

The authors declare that they have no conflict of interest related to the research, authorship, or publication of this article. No financial, personal, institutional, or professional relationships influenced the design of the study, analysis and interpretation of the results, or preparation of the manuscript.

Acknowledgement

The authors would like to express their sincere gratitude to the **Sekolah Tinggi Teknologi Angkatan Laut (STTAL), Surabaya, Indonesia**, for providing institutional support for this research. The authors also acknowledge the Indonesian Navy experts who contributed their professional knowledge and assessments during the Delphi and model-development processes. Their expertise and valuable insights were essential to the development and validation of the Smart Defense model.

REFERENCES

- Akdağ, M., Solnør, P., & Johansen, T. A. (2022). Collaborative collision avoidance for maritime autonomous surface ships: A review. *Ocean Engineering*, 250, 110920. <https://doi.org/10.1016/j.oceaneng.2022.110920>
- Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. *Ocean & Coastal Management*, 236, 106493. <https://doi.org/10.1016/j.ocecoaman.2023.106493>

- Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information*, 13(1), 22. <https://doi.org/10.3390/info13010022>
- 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. <https://doi.org/10.1016/j.ijcip.2022.100571>
- Bueger, C., & Edmunds, T. (2020). Blue crime: Conceptualising transnational organised crime at sea. *Marine Policy*, 119, 104067. <https://doi.org/10.1016/j.marpol.2020.104067>
- Bueger, C., Edmunds, T., & McCabe, R. (2020). Into the sea: Capacity-building innovations and the maritime security challenge. *Third World Quarterly*, 41(2), 228–246. <https://doi.org/10.1080/01436597.2019.1660632>
- Burmeister, H.-C., & Constapel, M. (2021). Autonomous collision avoidance at sea: A survey. *Frontiers in Robotics and AI*, 8, 739013. <https://doi.org/10.3389/frobt.2021.739013>
- Canepa, M., Ballini, F., Dalaklis, D., Vakili, S., & Hernandez, L. M. C. (2021). CR CyberMar as a solution path towards cybersecurity soundness in the maritime logistics domain. *Transactions on Maritime Science*, 10(1), 147–153. <https://doi.org/10.7225/toms.v10.n01.011>
- Darajati, M. R., & Syafei, M. (2022). Strategi pemberantasan praktik penangkapan ikan secara ilegal di wilayah laut Indonesia. *Jurnal Hukum IUS QUIA IUSTUM*, 30(1). <https://doi.org/10.20885/iustum.vol30.iss1.art7>
- Drazovich, L., Brew, L., & Wetzel, S. (2021). Advancing the state of maritime cybersecurity guidelines to improve the resilience of the maritime transportation system. In 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 503–509). IEEE. <https://doi.org/10.1109/CSR51186.2021.9527922>
- Erstad, E., Ostnes, R., & Lund, M. S. (2021). An operational approach to maritime cyber resilience. *TransNav*, 15(1), 27–34. <https://doi.org/10.12716/1001.15.01.01>
- Kanwal, K., Shi, W., Kontovas, C. A., Yang, Z., & Chang, C.-H. (2022). Maritime cybersecurity: Are onboard systems ready? *Maritime Policy & Management*, 51(3), 484–502. <https://doi.org/10.1080/03088839.2022.2124464>
- Karamperidis, S., Kapalidis, C., & Watson, T. (2021). Maritime cyber security: A global challenge tackled through distinct regional approaches. *Journal of Marine Science and Engineering*, 9(12), 1323. <https://doi.org/10.3390/jmse9121323>
- Kuhn, K., Bicakci, S., & Shaikh, S. A. (2021). COVID-19 digitization in maritime: Understanding cyber risks. *WMU Journal of Maritime Affairs*, 20(2), 193–214. <https://doi.org/10.1007/s13437-021-00235-1>
- Larsen, M. H., & Lund, M. S. (2021). Cyber risk perception in the maritime domain: A systematic literature review. *IEEE Access*, 9, 144895–144905. <https://doi.org/10.1109/ACCESS.2021.3122433>
- Liu, C., Chu, X., Wu, W., Li, S., He, Z., Zheng, M., Zhou, H., & Li, Z. (2022). Human–machine cooperation research for navigation of maritime autonomous surface ships: A

- review and consideration. *Ocean Engineering*, 246, 110555. <https://doi.org/10.1016/j.oceaneng.2022.110555>
- Meland, P. H., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents. *TransNav*, 15(3), 519–530. <https://doi.org/10.12716/1001.15.03.04>
- Park, C., Kontovas, C. A., Yang, Z., & Chang, C.-H. (2023). A BN-driven FMEA approach to assess maritime cybersecurity risks. *Ocean & Coastal Management*, 235, 106480. <https://doi.org/10.1016/j.ocecoaman.2023.106480>
- Pertiwi, S. B. (2020). Repositioning Indonesia in the changing maritime landscape of the Indo-Pacific region. *Global: Jurnal Politik Internasional*, 22(1), 1–25. <https://doi.org/10.7454/global.v22i1.438>
- Schinas, O., & Metzger, D. (2023). Cyber-seaworthiness: A critical review of the literature. *Marine Policy*, 151, 105592. <https://doi.org/10.1016/j.marpol.2023.105592>
- Taddeo, M., McNeish, D., Blanchard, A., & Edgar, E. (2021). Ethical principles for artificial intelligence in national defence. *Philosophy & Technology*, 34, 1707–1729. <https://doi.org/10.1007/s13347-021-00482-3>
- Tai, Z., Guo, J., Guan, Y., & Shi, Q. (2021). Impact of COVID-19 on port production and operation based on System Dynamics: A case study of Shanghai Port in China. *Journal of Advanced Transportation*, 2021, 9689391. <https://doi.org/10.1155/2021/9689391>
- Vagale, A., Oucheikh, R., Bye, R. T., Osen, O. L., & Fossen, T. I. (2021). Path planning and collision avoidance for autonomous surface vehicles I: A review. *Journal of Marine Science and Technology*, 26, 1292–1306. <https://doi.org/10.1007/s00773-020-00787-6>
- Zhang, X., Wang, C., Jiang, L., An, L., & Yang, R. (2021). Collision-avoidance navigation systems for Maritime Autonomous Surface Ships: A state-of-the-art survey. *Ocean Engineering*, 235, 109380. <https://doi.org/10.1016/j.oceaneng.2021.109380>
- Ziajka-Poznańska, E., & Montewka, J. (2021). Costs and benefits of autonomous shipping—A literature review. *Applied Sciences*, 11(10), 4553. <https://doi.org/10.3390/app11104553>