An Assessment of Cyber Resilience in the Maritime Domain Using System Dynamics and Analytical Hierarchy Process (AHP)

I Nengah Putra[1], Amarulla Octavian[1], April Kukuh Susilo[2], Y N Santosa[3]

The maritime industry is increasingly dependent on digital technology, making it vulnerable to cyber threats. Every stakeholder is exposed to cybersecurity risks and challenges. This research aims to provide an assessment and simulation model of cyber resilience in the maritime domain, supported by qualitative descriptive statistical methods. This study is also supported by system dynamics and Analytical Hierarchy Process (AHP). The data were obtained from an eight-member expert panel (academics and practitioners) and pertain to the research period January 2022 – February 2023 and the Indonesian Sea area. Research results on global weight revealed the threat (MC-1), vulnerability (MC-2), and technologies (MC-3) sub-criteria as the most important, with the global weight of 0.102 each, followed by the navigation (MO-2), and governance and compliance (CR-6) sub-criteria with the global weight of 0.072 and 0.065, respectively. Maritime cyber resilience evaluation is based on three main criteria. The maritime operation criterion has the highest resilience value, with overall evaluated value of maritime cyber resilience being in the acceptance resilience category level 4, with the value of 3.535 (70.701%). Furthermore, changes in the maritime cyber resilience value in the 2022-2025 period are still at level 4 (acceptance resilience). Maritime cyber resilience is expected to stagnate at its current level 4 in 2023. In the third and fourth year (2024-2025), a downward trend in the maritime cyber resilience value is expected.

KEY WORDS
~ Maritime cyber
~ Analytical Hierarchy Process (AHP)
~ Cybersecurity
~ Maritime operation
~ System dynamics
~ Resilience

[1] Indonesia Defense University, Citeureup-Bogor, Indonesia
[2] Airlangga University, Surabaya, East Java, Indonesia
[3] Indonesia Naval Technology College, Surabaya, East Java, Indonesia
e-mail: april.kukuh.susilo-2020@feb.unair.ac.id

doi: 10.7225/toms.v13.n02.w06

Received: 26 Apr 2024 / Revised: 24 Mar 2024 / Accepted: 11 Jun 2024 / Published online: 20 Jun 2024

This work is licensed under

1. INTRODUCTION

The maritime sector has been increasingly relying on digital technology, rendering it vulnerable to cyber attacks (Erstad et al., 2023). The consequences of cyberattacks on the maritime industry can be dire, ranging from financial losses to environmental disasters (Akpan et al., 2022). One of the main challenges in achieving maritime cyber resilience is the complexity of the maritime ecosystem, which involves various stakeholders, including ship owners, port authorities, shipping companies, and governmental agencies (Park et al., 2019). All stakeholders are exposed to cybersecurity risks and challenges that must be overcome (Drazovich, Brew and Wetzel, 2021).

Cyber resilience is a new strategy used to address this issue. From an organizational, technological, and human perspective, this strategy is often described as the capacity to foresee, detect, contain, develop, and recover from a cyber incident (Carías et al., 2020). Sharing information about cyber incidents raises awareness, reduces vulnerability, helps manage risks, and improves cyber resilience (Oruc, 2022). It should also incorporate a resilience strategy that addresses cyber response and recovery plans, as well as recommendations for systems that increase cyber resilience (Drazovich, Brew and Wetzel, 2021).

Malatji et al. (2022) explain the need for future research on the implementation of cybersecurity capability frameworks, and propose concepts and methods (Roege et al., 2017) to measure the level of cyber resilience (Gu and Liu, 2022). Estay (2021) conveys the need for dynamic model-based research to take into account different levels and network hierarchies in cyber resilience. According to Park et al. (2023), further research on cybersecurity and resilience evaluation (Hausken, 2020) in the maritime industry is needed to mitigate cyber threats (Afenyo and Caesar, 2023). Therefore, cybersecurity in the marine sector needs to be assessed by considering the idea and application of network hierarchy.

The purpose of this study was to evaluate cyber resilience in the maritime industry and simulate it using a model. A qualitative descriptive statistical method and the system dynamics method with Stella 9 and the Analytical Hierarchy Process (AHP) were used by an eight-member expert panel (academics and practitioners) in the January 2022 – February 2023 research period. The Indonesian Sea area was the locus of research as a cross-economic world maritime pathway (Susilo et al., 2019).

This research is important for identifying vulnerabilities and potential risks to the maritime industry's critical infrastructure. By assessing cyber resilience, stakeholders can identify areas most vulnerable to cyber threats and develop risk mitigation strategies. Assessing cyber resilience in the maritime industry helps stakeholders comply with guidelines and regulations with respect to factors to be aware of and prioritize. By demonstrating a commitment to cybersecurity and resilience, stakeholders can build trust among themselves and with customers who rely on maritime services.

The research has several contributions. First, it broadens the study of literature from the maritime context (Gunes, Kayisoglu and Bolat, 2021), especially in the field of maritime cyber management. Second, this study offers a paradigm for evaluating cyber resilience in the maritime industry to reduce and mitigate cyber hazards (Kulugh, Mbanaso and Chukwudebe, 2022). Third, it gives an overview of maritime organizations to help them improve their overall cyber security posture and reduce the risk of cyberattacks (Noor, 2022) by identifying vulnerabilities, developing effective countermeasures, integrating smart ports and digital solutions in the maritime industry, and improving cybersecurity standards.

This research is structured as follows: Section 2 gives an overview of the relevant research literature on cyber resilience, maritime cybersecurity (Mcs), maritime cyber resilience. Section 3 explains the methodology used, from the conceptual framework, identification of key variables in maritime cyber resilience to causal loop diagrams, and stock flow diagrams. Section 4 gives the results, discussion and implications. Section 5 is the conclusion of the research, limitations and future research.

2. LITERATURE OVERVIEW

2.1. Cyber resilience

The ability to fend off cyberattacks and reduce risks is referred to as cyber resilience. Local and global economies must maximize the value of technological innovation (Peter, 2017). This condition involves a combination of technical measures, policies, procedures, and training designed to help organizations maintain their critical operations and services in the face of cyber threats (Steingartner, Galinec and Kozina, 2021). Cyber resilience is different from cybersecurity which usually focuses on preventing cyberattacks (Carías et al., 2019). Cyber resilience recognizes that cyberattacks are unavoidable and that organizations need to be prepared to respond quickly and effectively when they occur (Erstad et al., 2023).

There are several key components of cyber resilience (Drazovich, Brew and Wetzel, 2021). First, organizations need to have a comprehensive understanding of IT infrastructure and the potential risks (Hausken, 2020). Second, organizations need to have an effective incident response plan (Steingartner, Galinec and Kozina, 2021). Third, organizations need to have strong backup and recovery capabilities (Carías et al., 2019). Overall, cyber resilience is an important component of any organization's security posture. By taking a proactive approach to prepare for cyber-attacks and other security incidents, organizations can minimize the impact of these events on their operations and services (Hausken, 2020). Cyber resilience theory can also be developed through empirical quantification of an organization's cyber resilience, through case studies and stress testing of organizations with techniques such as non-invasive games.

At each of these levels, cyber resilience can be attained or compromised. Actors can be self-serving, altruistic, or charitable, for example. Individuals, workers, citizens, entrepreneurs, developers, consumers, producers, manufacturers, system integrators, cybersecurity providers, environmentalists, philanthropists, representatives, elected officials, stakeholders, organizations, interest groups, idealistic organizations, non-profits, governmental units, governments, countries, union of countries, profit organizations, firms, businesses, and enterprises are examples of actors. Insofar as they want to build cyber resilience, these entities are not threats.

Estay (2021) explains cyber resilience of a system exposed to malware cyberattacks. Erstad et al. (2023) explains the effectiveness of implementing HCD when designing maritime cyber resilience training. Carías et al. (2019), developed a system dynamics model that represents the theoretical behavior of the variables involved in managing cyber resilience. In this research, cyber resilience theory is applied to maritime cyber security using a system modeling approach.

2.2. Maritime cybersecurity (MCS)

Cybersecurity is a relatively new and as yet poorly understood concept in shipping, with the majority of maritime operators and managers having completed no cyber risk training (Kechagias *et al.*, 2022). Maritime cybersecurity can be defined as part of maritime security which is concerned with protecting against cyber threats from all aspects of maritime cyber systems and maritime cybersecurity which is concerned with reducing the consequences of cyberattacks on maritime operations (Erstad, Ostnes and Lund, 2021). Maritime cybersecurity is a combination of the terms 'maritime security' and 'cybersecurity.' It has been argued that maritime security has no definite meaning, and is further related to different concepts depending on the individual trying to understand it or put it into practice (Bueger, 2015).

As assets in the maritime domain become more integrated with increased information sharing between ICT systems, maritime security is coming to depend on a mature understanding of cybersecurity to operate and navigate safely and securely (Hareide *et al.*, 2018). Based on a thorough survey of relevant literature, there are six critical dimensions which are categorized as the basis that affects maritime cybersecurity performance (Kanwal *et al.*, 2022), namely, the regulatory framework; cybersecurity-related company procedures; ship systems readiness; cyber training and awareness; compliance monitoring; human factors.

2.3. Maritime cyber resilience

Maritime operations are activities at sea that must be carried out without companies losing control, so they can keep performing them and recovering in the face of challenges (Erstad et al., 2021). Maritime cyber resilience originally appeared as a part of maritime cyber risk management. Students need to develop their collaborative and teamwork skills since maritime cyber risk management is an interdisciplinary subject that encompasses resilience, safety, and maritime cybersecurity (Erstad et al., 2023). As maritime cybersecurity places a focus on the capacity to foresee, contain, recover from cyber threats and evolve in the shortest amount of time (Erstad et al., 2021), it is a unifying idea that contributes to our understanding of maritime cyber risk management. Maritime cyber resilience has been defined as the ability of maritime systems to learn how to maintain and develop regular operations, as well as anticipate, contain, recover from, and adapt to cyber threats rapidly (Erstad et al., 2021).

According to Erstad et al. (2021), studies dealing with maritime cyber resilience should focus on navigators because they are on the cutting edge of operations, perhaps being the only agents capable of detecting undesired variations. In addition, if technology fails, the navigator is expected to take control. When discussing maritime cyber resilience, one underlying presumption is that navigators must acknowledge that the security of the situation can be regulated and will eventually be effectively controlled.

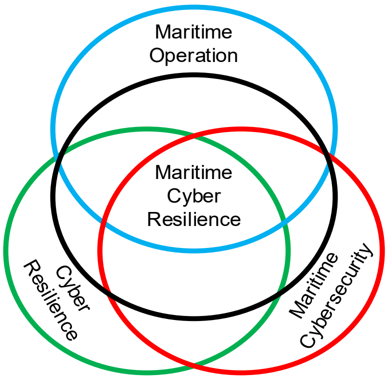

Figure 1. Origins of maritime cyber resilience, adapted from Erstad et al. (2021)

3. METHODOLOGY

This study uses a qualitative descriptive statistical approach. The descriptive statistical qualitative design was used at different times and sequentially, starting with qualitative research and then supported by data in the form of statistical figures (Hanson et al., 2005; Taguchi, 2018). This study discusses the complexities of integrating cyber resilience into the maritime domain using system dynamics. This complexity is addressed by formulating causal CLDs (strengthening and balancing) to demonstrate qualitative impacts. After that, SD modeling and simulation were used to assess cyber resilience with qualitative scores in system modeling. The research was supported by the AHP method and system dynamics approach, Microsoft Office and Stella 9. The AHP method was used to conduct a weighting analysis of maritime cyber resilience factors and sub-factors and as an initial stage of cyber resilience assessment. System dynamics was used in sustainability analysis on maritime cyber resilience over a period of five years.

Primary and secondary data were collected for the needs of this research. Primary data were obtained from cyber experts ranging from practitioners to academics. The expert selection criteria were as follows: 1) academics with a minimum masters degree (Hult Khazaie and Khan, 2020; Rioja-Lang et al., 2020); 2) practitioners working with maritime cyber resilience (Fallah and Ocampo, 2021); 3) over five years of work experience (Khalilzadeh, Katoueizadeh and Zavadskas, 2020; Kim and Kim, 2022); 4) eight expert members (5 practitioners, 3 academics) based on Almanasreh et al. (2019). Secondary data include news and information from print media, research findings from internet media, archive materials, rules and policies, official institutional documents, and official social media profiles.

The study was conducted in Jakarta and other Indonesian international port cities that represent maritime cyber resilience, namely Medan, Semarang, Surabaya and Makasar. These cities were chosen because they are large port cities in Indonesia which have all port complexities and standards. On the other side, Indonesia was chosen due to its strategic geographical position and the sea serving as the main transportation route. The research was conducted from January 2022 to February 2023 by means of a questionnaire for experts based on secondary data. Observations with respect to the assessment of maritime cyber resilience have been a concern of researchers for a long time. In Indonesia itself, the study of maritime cyber resilience, which is vulnerable to cyberattacks, is a serious study. Therefore, researchers saw an opportunity to provide theoretical contributions to research in the area of maritime cyber resilience.

3.1. Conceptual framework

In this study, which is divided into three parts, the resilience of the maritime cyber domain, which is situated in the Indonesian Sea area, is specifically discussed. First, prior research was studied, questionnaire-based brainstorming conducted, and expert opinions obtained to identify crucial elements and examine the relationships between variables in maritime cyber resilience. Second, the assessment and weighting of maritime cyber resilience were used in the measurement. This weighting was performed using the AHP method, and the information were collected from experts carefully selected among important stakeholders. Score assessment was also carried out using the Likert scale. The function of the AHP method in this research is not only to weight sub-factors but also to provide a resilience assessment at the next stage. Third, this discussion examined how system dynamics modeling can be used to assess the benefits of maritime cyber resilience.

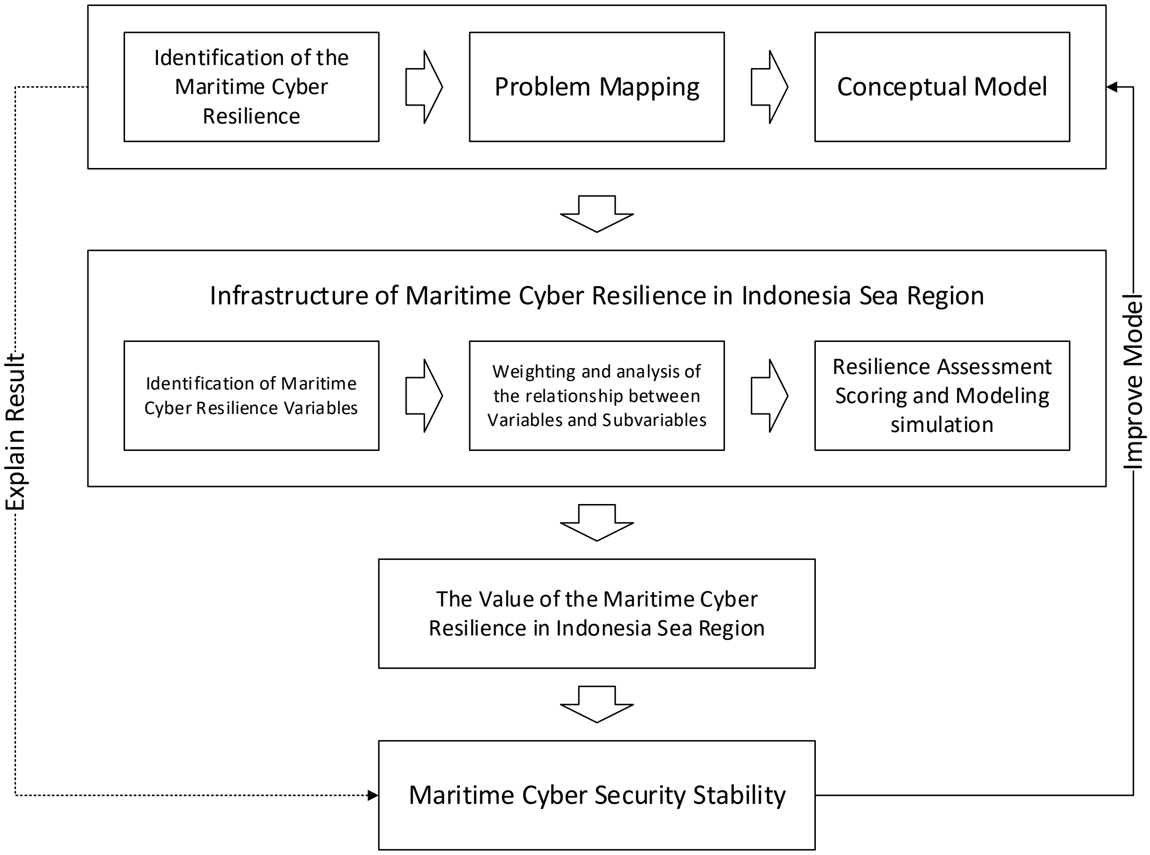
Identification of the Maritime Cyber Resilience
Problem Mapping
Conceptual Model
Infrastructure of Maritime Cyber Resilience in Indonesia Sea Region
Identification of Maritime Cyber Resilience Variables
Weighting and analysis of the relationship between Variables and Subvariables
Resilience Assessment Scoring and Modeling simulation
The Value of the Maritime Cyber Resilience in Indonesia Sea Region
Maritime Cyber Security Stability
Explain Result
Improve Model

Figure 2. A conceptual framework for evaluating maritime cyber resilience

In assessing the cyber maritime resilience analysis, the average score of the resilience dimension across all sub-variables in the identified variables was calculated. Second, calculated overall robustness rating for each variable and sub-variables was weighted as determined by the experts. All of the factors and sub-variables should receive equal weight from these experts. Therefore, the resistance rating was calculated as follows, based on research by Herrera (2017), Mbanaso et al. (2019) and Li et al. (2020).

$$\text{Resilience Index} = \frac{(\text{Variable 1}*\text{weight})+(\text{Variable 2}*\text{Weight})+(\text{Variabel x}*\text{weigth})}{100} \qquad \text{(Eq. 1)}$$

Scale AHP	Description	Likert	Resilience
9	Baseline security; the best practice value	5	Fully achieved
7-8	Controls that are implemented structurally but are inconsistent; only a few minor elements are absent	4	Largely achieved
5-6	There are some controls in place, but they are not consistently and structurally ordered, and there are several and/or significant aspects absent	3	Partially achieved
3-4	few controls in place or incoherent controls	2	Loosely achieved
1-2	lack of controls or ineffective controls	1	Not achieved

Table 1. AHP scale values and Likert scores and resilience category values Sources: Aksha et al. (2019); Rehak et al. (2019); Octavian et al. (2021)

Level	Score	Percent (%)	Resilience Level	Description
5	4.01-5	81-100	High resilience	There is no need to take any additional measures because the measurable elements in this category have outstanding specifications.
4	3.01-4	61-80	Acceptable resilience	The measurable items in this category have extremely good parameters that can still be improved upon, but these improvements are not required for the overall element resilience level.
3	2.01-3	41-60	Low resilience	The measured criteria in this category are adequate, but their enhancement would significantly increase the resistance of the element.
2	1.01-2	21-40	Insufficient resilience	The measurable elements in this category have extremely subpar properties, which significantly weaken the robustness of the variable to which they belong.
1	0-1	0-20	Critical resilience	These quantifiable items either don't exist or have alarmingly low parameters. They must be completely altered, and the process of adjusting and restoring them must begin right away.

Table 2. Maritime cyber resilience

3.2. Identification of key variables in maritime cyber resilience

The identification of key variables is an important step in research or analysis. Important elements are those that significantly affect maritime cyber resilience. These variables can be identified by reviewing existing literature, consulting with experts in the field, or by exploratory research. Key variables are variables that have a significant impact on research results and are highly important for understanding the phenomenon of maritime cyber resilience.

Maritime cyber resilience refers to the ability of the maritime industry to protect its critical systems and infrastructure from cyber threats, detect and respond to cyber incidents, and quickly recover from any disruptions caused by those incidents. The identification of key variables that impact resilience is paramount for improving maritime cyber resilience. This paper takes into account the context and framework established by the study's primary goal, which is to be able to identify areas of maritime cybersecurity. Some adjustments must be made to fit this context when choosing the variables to be used as indicators. The factors that are present in the context of resilience generally have, therefore, not been regarded as representative and have been disregarded or replaced with other, more pertinent variables. In this research, the strategy was to rely on expert judgment to broaden the validation of the empirical determination of the indicators, as explained above. In terms of maritime cyber resilience in the Indonesian Sea region, each expert was asked to indicate his area of expertise. Experts have confirmed some of the suggested markers, such as:

Variables	Sub-variables	Coding	References
Cyber Resilience (CR)	Threat intelligence	CR-1	(Jacq et al., 2019; Mbanaso, Abrahams and Apene, 2019)
	Risk assessment	CR-2	(Tam and Jones, 2018; Mraković and Vojinović, 2019; Leite Junior et al., 2021)
	Prevention and protection	CR-3	(Roege et al., 2017; Dolezal and Tomaskova, 2018)
	Detection and response	CR-4	(Mbanaso, Abrahams and Apene, 2019; Lee, Huh and Kim, 2020)
	Recovery and continuity	CR-5	(Kolini and Janczewski, 2015; Razikin and Soewito, 2022)
	Governance and compliance	CR-6	(Jovanović et al., 2020; Tam et al., 2023)
Maritime Operation (MO)	Vessel design	MO-1	(McGillivary, 2018; Caprolu et al., 2020)
	Navigation	MO-2	(Boyes, 2014; Enoch, Lee and Kim, 2021; Freire et al., 2022)
	Cargo handling	MO-3	(Gunes, Kayisoglu and Bolat, 2021; Melnyk et al., 2022)
	Safety	MO-4	(Greiman, 2020; Erstad et al., 2023)
	Security	MO-5	(Khalid Khan, Shiwakoti and Stasinopoulos, 2022; Park et al., 2023)
	Environmental protection	MO-6	(Mraković and Vojinović, 2019; Androjna and Perkovič, 2021; Kanwal et al., 2022)
	International regulations	MO-7	(Ding et al., 2022; Kapalidis et al., 2022)
Maritime Cybersecurity (MC)	Threats	MC-1	(Jones, Tam and Papadaki, 2016; Ghelani, 2022; Afenyo and Caesar, 2023)
	Vulnerabilities	MC-2	(Tweneboah-Koduah, Skouby and Tadayoni, 2017; Seetharaman et al., 2021; Yaacoub et al., 2022)
	Regulations	MC-3	(Gunes, Kayisoglu and Bolat, 2021; Kotis, Stavrinos and Kalloniatis, 2023; Park et al., 2023)
	Technologies	MC-4	(Gunes, Kayisoglu and Bolat, 2021; Raicu and Raicu, 2021; Erstad et al., 2023)
	Collaboration	MC-5	(Wahl, 2020; Androjna and Perkovič, 2021; Progoulakis et al., 2021)

Table 3. Selected maritime cyber resilience assessment variables

To analyze maritime cyber resilience factors and clarify the relationships between the main variables in the system, a causal loop diagram (CLD) was developed, which presents the qualitative relationships that occur in a complex system and makes it possible to infer the tendency of the system to grow or shrink; and stock and flow diagrams/models (hard modeling), which represent quantitative relationships.

Although CLD can describe the basic structure of feedback relationships, it cannot distinguish the differences between various variables. Therefore, a flow diagram (FD) was developed to explain the accumulation of reactions for different variable levels. Building causal relationships between variables and sub-variables using stock flow diagrams was the next step in establishing relationships between variables and sub-variables. Establishing a quantitative model for model simulation was the goal of this stage. To enable the operation of a simulation program, the modeling required that every relationship between variables and system components be converted to mathematical equations.

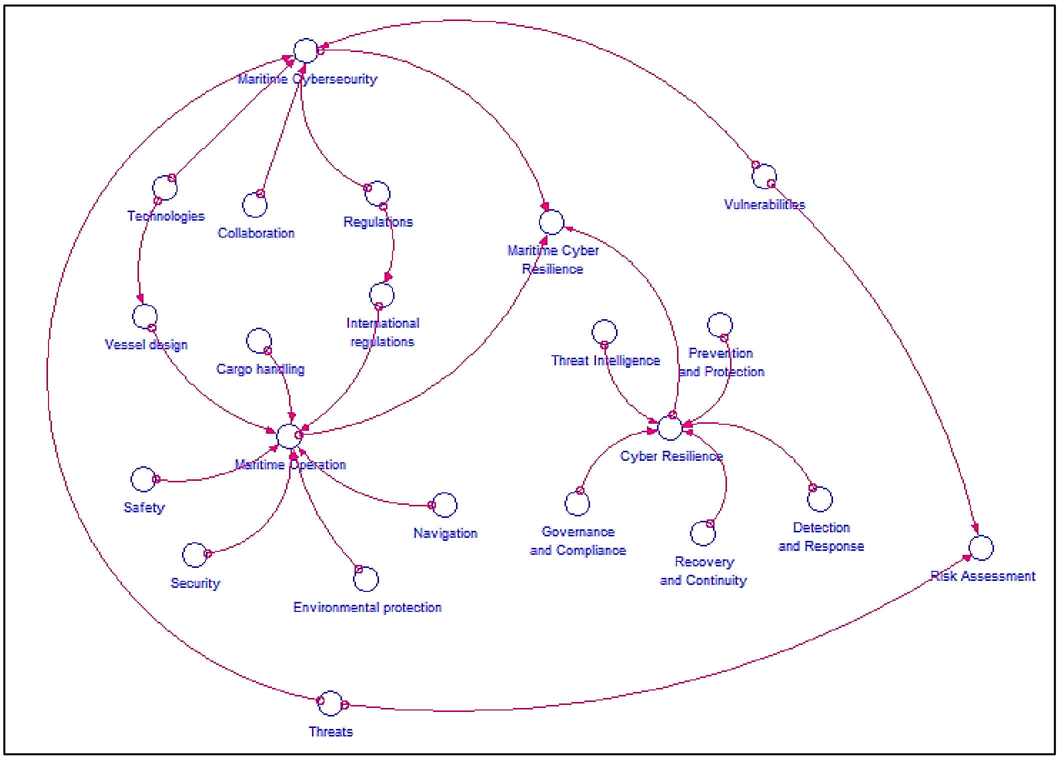

Figure 3. Causal loop diagram for maritime cyber resilience

A quantitative model was created by determining the general quantitative framework, fundamental time units for the simulation, functional forms of the model equations, estimating their parameters, inputting the equations into the simulation program, running the reference simulation, and establishing the model equations. This stage relied on validated professional judgment. The results of the relationship analysis are presented in Figure 6.

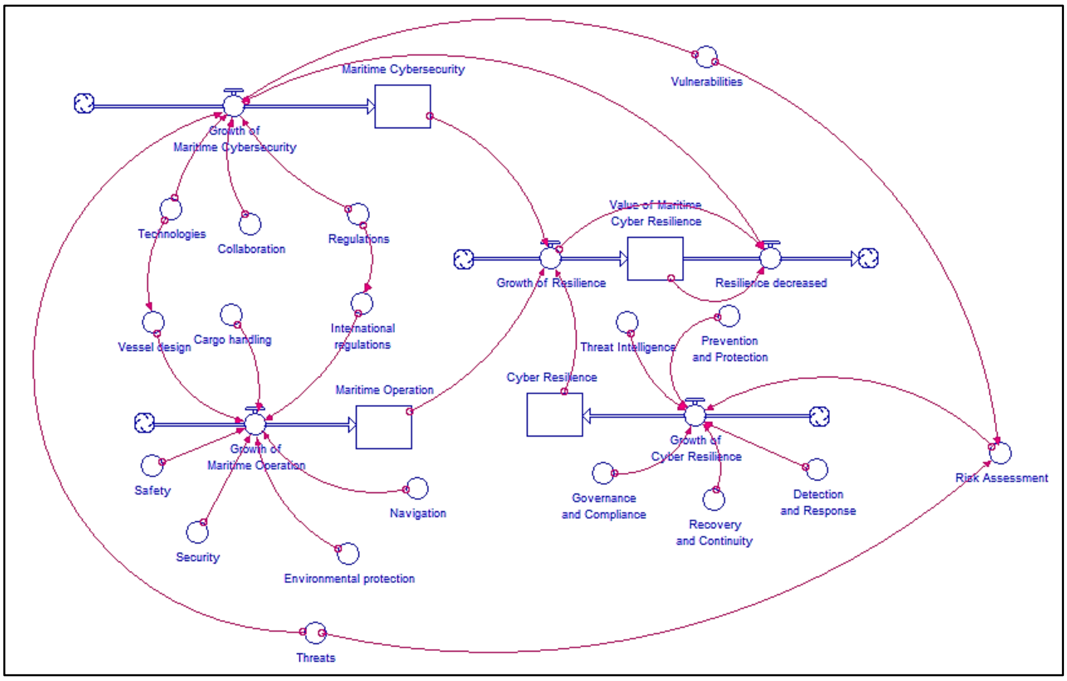

Figure 4. Stock flow diagram of maritime cyber resilience

The goals and scenarios of each model were used to evaluate the modeling system dynamics of maritime cyber resilience. The scenarios were assumed to be the outcome of a simulation where no effort or intervention were made to improve maritime cyber security. This illustrates that maritime cyber relations, predictions and their impact on resilience in the 2022-2025 period have been closely related to Cyber Resilience (CR), Maritime Operations (MO), and Maritime Cybersecurity (MC). The model development process involves the identification of behavior patterns and correlations between variables that affect how well the model represents reality (Octavian et al., 2021).

4. RESULT AND DISCUSSION

4.1. Variable and sub-variable weighting

Each expert was then asked to consider the key indicators believed to be the most important for defining or forecasting maritime cyber resilience, and, based on their experience in different areas of cyber maritime resilience assessment, rank the various indicators by importance. Multiple ranking activities can be carried out by experts. The ability to distinguish between the primary indicators of cyber maritime resilience was another question posed to the experts. The Analytical Hierarchy Process (AHP) approach was used for weighting, which had a time scale based on the standards for the link between variables and sub-variables.

Depending on the study subject, this model will produce a different output, which will be a vector comprising the local weights of the options taken into consideration for each sub-criterion. The global vectors containing the weights for the higher-level criteria are multiplied by the local vectors containing the weights for these sub-criteria after normalization (parent criteria), and the final vector of decision problems will be obtained, as in research by Improta et al., (2018). In summary, as in system dynamics modeling, every criterion in the hierarchy is simulated, taking into account all the relationships between the sub-criteria linked to the same parent criterion, as well as their variability over time.

Specific decision vectors can be derived at each time step of the simulation process by the weighted scenario evaluation criteria. By doing so, the static behavior of conventional AHP approaches can be replaced with time-varying decision-making processes. Each criterion and sub-criterion is inserted in the AHP formula, and the results are compared against those of the simulation produced by the model. The decision-making process enables value and scenario evaluation, or the selection of the ideal set of parameters. The results of the weighting are presented in Figure 5 and Table 7.

Criteria	CR	MO	MC	weight
CR	1	1	1/2	0.261
MO	1	1	1	0.328
MC	2	1	1	0.411
CR=	0.046			1.000

Table 4. Pairwise comparison matrix aggregation for Maritime Cyber Resilience

Criteria	CR-1	CR-2	CR-3	CR-4	CR-5	CR-6	Weight
CR-1	1	1	2	2	2	1/2	0.198
CR-2	1	1	1	2	1	1	0.177
CR-3	1/2	1	1	1	2	1/2	0.144
CR-4	1/2	1/2	1	1	1/2	1/2	0.100
CR-5	1/2	1	1/2	2	1	1/2	0.130
CR-6	2	1	2	2	2	1	0.250
CR =	0.040						1.000

Table 5. Pairwise comparison matrix aggregation for Cyber Resilience variable

Criteria	MO-1	MO-2	MO-3	MO-4	MO-5	MO-6	MO-7	Weight
MO-1	1	1	2	1	1	2	2	0.179
MO-2	1	1	2	2	2	2	2	0.219
MO-3	1/2	1/2	1	1/2	1	1/2	1	0.091
MO-4	1	1/2	2	1	2	2	2	0.180
MO-5	1	1/2	1	1/2	1	1	2	0.124
MO-6	1/2	1/2	2	1/2	1	1	1/2	0.104
MO-7	1/2	1/2	1	1/2	1/2	2	1	0.103
CR =	**0.035**							**1.000**

Table 6. Pairwise comparison matrix aggregation for Maritime Operation variable

Criteria	MC-1	MC-2	MC-3	MC-4	MC-5	Weight
MC-1	1	1	2	1	2	0.248
MC-2	1	1	2	1	2	0.248
MC-3	1/2	1/2	1	1/2	1/2	0.111
MC-4	1	1	2	1	2	0.248
MC-5	1/2	1/2	2	1/2	1	0.146
CR =	0.013					1.000

Table 7. Pairwise comparison matrix aggregation for Maritime Cybersecurity variable

Table 4 shows that Maritime Cybersecurity (MC) variable, with the weight value of 0.4111, should be prioritized, followed by the Maritime Operation (MO) variable, with the weight of 0.3278 and third, the Cyber Resilience (CR) variable, with the weight of 0.2611. Maritime cybersecurity has attracted increasing, accelerating attention in recent years (Oruc, 2022), requires a holistic strategy due to the maritime industry's growing system complexity, digitization, and automation (Mraković and Vojinović, 2019), and is an issue that requires immediate attention (Karamperidis, Kapalidis and Watson, 2021). Collaboration between business, government, and academics may dramatically and effectively boost maritime cybersecurity performance (Kanwal et al., 2022). On the other hand, private companies need to dedicate a large part of their budget to addressing maritime cybersecurity issues (Afenyo and Caesar, 2023). To ensure the safe operation of ships and improve the security of the maritime environment, scientists contribute to the development and implementation of maritime cybersecurity methods and policies (McGillivary, 2018). Therefore, the aspect of maritime cybersecurity is the most influential variable in maritime cyber resilience.

The Cyber Resilience aspect in Table 8 shows that the Governance and Compliance (CR-6) sub-variable is top priority with the highest weight of 0.250, while the Detection and Response (CR-4) sub-variable has the lowest weight of 0.026. For Aspects of Maritime Operations (MO), in Table 9, the Navigation sub-variable (MO-2) is a top priority with the highest weight of 0.219, while the Cargo handling sub-variable (MO-3) has the lowest weight, namely 0.03. Furthermore, the Maritime Cybersecurity (MC) aspect in Table 10 shows the Threat (MC-1), Vulnerability (MC-2), and Technologies (MC-4) sub-variables each have weight of 0.248 as the highest weight value.

4.2. Consistent test results

Before establishing the overall weight of each variable/criteria, a comparison matrix consistency test was performed for each technique to determine the consistency of the data from the completed questionnaire. In the AHP method, consistency test is known as the CR (Consistency Ratio). If the CR value is under 0.1, the data are considered consistent; if it is greater than 0.1, the data are considered inconsistent (Sharma et al., 2019; Arora et al., 2020; Maletič et al., 2021). The calculation results show that each variable and sub-variable passed the consistency test using the AHP approach (Table 4; Table 5; Table 6; Table 7) and had the CR value <0.1; therefore, pairwise comparison results were seen to be consistent.

Variables	Weight	Sub-variables	Coding	Local weight	Overall weight	Rank
Cyber Resilience (CR)	0.2611	Threat Intelligence	CR-1	0.198	0.052	9
		Risk Assessment	CR-2	0.177	0.046	10
		Prevention and Protection	CR-3	0.144	0.038	13
		Detection and Response	CR-4	0.100	0.026	18
		Recovery and Continuity	CR-5	0.130	0.034	15
		Governance and Compliance	CR-6	0.250	0.065	5
Maritime Operation (MO)	0.3278	Vessel design	MO-1	0.179	0.059	8
		Navigation	MO-2	0.219	0.072	4
		Cargo handling	MO-3	0.091	0.030	17
		Safety	MO-4	0.180	0.059	7
		Security	MO-5	0.124	0.041	12
		Environmental protection	MO-6	0.104	0.034	14
		International regulations	MO-7	0.103	0.034	16
Maritime Cybersecurity (MC)	0.4111	Threats	MC-1	0.248	0.102	1
		Vulnerabilities	MC-2	0.248	0.102	1
		Regulations	MC-3	0.111	0.045	11
		Technologies	MC-4	0.248	0.102	1
		Collaboration	MC-5	0.146	0.060	6

Table 8. Each variable and dependent variable in maritime cybersecurity has local weight and global weight

Factor and sub-factor local and global weights are shown in Table 8. Evaluations of intangible qualitative criteria, as well as tangible quantitative criteria, might be included in the AHP process. Pairwise comparisons of each primary criterion and a number of its sub-criteria were used. The global weight of the sub-criteria was determined by multiplying the local weight of the sub-criteria with the weight of the major criterion, following pairwise comparisons of the main criteria and sub-criteria. Weights were calculated in four steps, after which local weights and global weights were calculated. Local weights indicate the relative importance of factors within the group, while global weights show the priority of factors with respect to maritime cyber resilience. Conclusions on the importance of the sub-criteria based on the perceptions of decision-makers can be drawn from this overall weight (Sharma et al., 2019). In practice, weights can be obtained, for instance, by directly asking for weights. In this situation, there was a need to ensure the weights also account for the range of criterion values, as in research by Mustajoki et al. (2020).

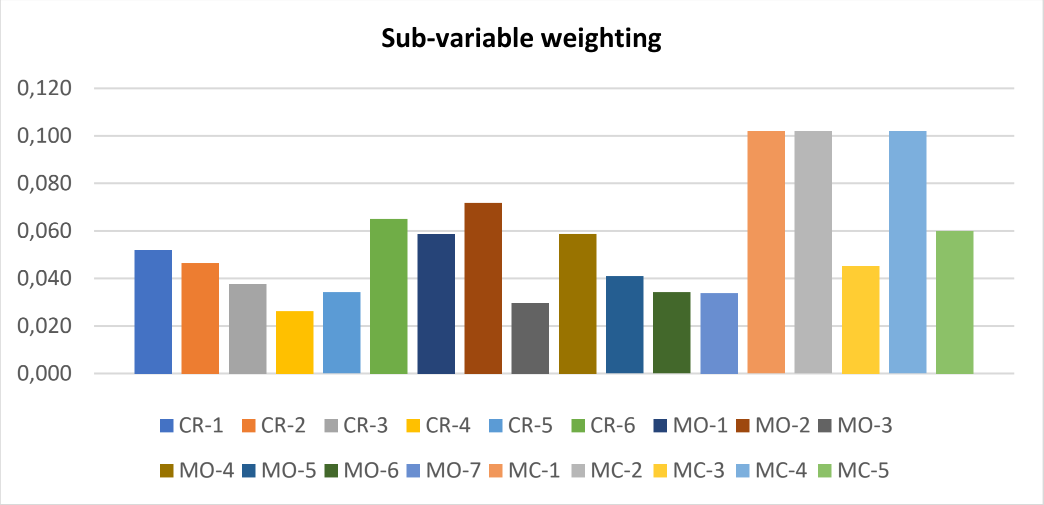

Figure 5. Global weight of sub-variable maritime cyber resilience

Table 8 and Figure 5 depict local and global weights and the overall ranking of each of the main criteria and sub-criteria. The results of the AHP methodology applied to global weights revealed that the threat (MC-1), vulnerability (MC-2), and technologies (MC-3) sub-criteria were considered the most important, with the global weight of 0.102 each, followed by the navigation (MO-2), governance and compliance (CR-6) with the global weight of 0.072 and 0.065, respectively. The detection and response (CR-4) sub-criterion ranked last in the pairwise comparisons.

The complexity of digital systems has been increasing due to the rapid and continuous advancement and development of information technology which has made systems less safe, and complicated and changed the nature of cyber threats (Aljuhami and Bamasoud, 2021). Organizational resilience is the capacity of an organization to resist failure to meet potential challenges, endure, and prosper (Steingartner, Galinec and Kozina, 2021). Internet-connected onboard workstations using Microsoft Windows and Microsoft Office have built-in vulnerabilities (Shahzad, Awan and Ghamdi, 2019). Fundamental research is needed in this field to address security vulnerabilities effectively (Humayun et al., 2020). By establishing an effective governance framework and ensuring compliance with relevant regulations, maritime organizations can better manage cybersecurity risks and protect themselves against cyber threats (Rios Insua et al., 2021).

4.3. Assessment of maritime cyber resilience

A simulation model was used to conduct the maritime cyber resilience evaluation. The values of the choice problem variables and sub-variables were input in the created model using the AHP weighting approach and a

Likert scale evaluation. A simulation model can be developed for each criterion in the dynamic system hierarchy as well. Each simulation model uses a vector as its input, and the size of the vector depends on how many options the decision question is examining. Vector rows are alternatives or preferences related to the choice problem, and each row provides all pertinent information for that alternative (Octavian et al., 2021). A model simulation is given in Figure 4. The primary objective of the simulation model was to enable the assessments of maritime cyber resilience. Model simulation results are provided in Figure 6.

Sub-variables	Weight	Score	Result	%	Explanation
Threat intelligence	0.198	3.397	0.674	67.946	Acceptable resilience
Risk assessment	0.177	3.552	0.630	71.047	Acceptable resilience
Prevention and protection	0.144	3.529	0.510	70.590	Acceptable resilience
Detection and response	0.100	3.594	0.359	71.889	Acceptable resilience
Recovery and continuity	0.130	3.792	0.494	75.836	Acceptable resilience
Governance and compliance	0.250	3.552	0.887	71.047	Acceptable resilience
Cyber resilience (CR)	1.000		**3.554**	71.074	Acceptable resilience

Table 9. Maritime cyber resilience evaluated values for cyber resilience (CR) criteria

The evaluation of maritime cyber resilience in the cyber resilience (CR) criteria consists of six sub-criteria, namely the Threat Intelligence (CR-1) sub-criteria with a resilience value of 0.674 (67.946%). The risk assessment sub-criterion (CR-2) has a resistance value of 0.630 (71.047%). The prevention and protection sub-criterion (CR-3) has a resistance value of 0.510 (70.59%). The detection and response (CR-4) sub-criteria has a resistance value of 0.359 (71.89%). The recovery and continuity sub-criterion (CR-5) has an endurance value of 0.494 (75.836%). The governance and compliance sub-criterion (CR-6) has a resilience value of 0.887 (71.047%). All sub-criteria in cyber resilience fall into the acceptable category, namely at level 4.

Sub-variables	Weight	Score	Result	%	Explanation
Vessel design	0.179	3.852	0.689	77.048	Acceptable resilience
Navigation	0.219	3.893	0.854	77.864	Acceptable resilience
Cargo handling	0.091	3.902	0.355	78.049	Acceptable resilience
Safety	0.180	4.156	0.747	83.113	High resilience
Security	0.124	3.618	0.450	72.354	Acceptable resilience
Environmental protection	0.104	3.618	0.376	72.354	Acceptable resilience
International regulations	0.103	3.538	0.364	70.757	Acceptable resilience
Maritime operation (MO)	1.000		**3.834**	76.688	Acceptable resilience

Table 10. Evaluated values of maritime cyber resilience for maritime operation (MO) criteria

The evaluation of maritime cyber resilience in the maritime operation (MO) criteria consists of seven sub-criteria, namely the vessel design sub-criteria (MO-1) with the resilience value of 0.689 (77.048%). Navigation sub-criterion (MO-2) had an endurance value of 0.854 (77.864%). The cargo handling sub-criterion (MO-3) had the endurance value of 0.355 (78.049%). The safety sub-criterion (MO-4) had the endurance value of 0.747

(83.113%). The security sub-criterion (MO-5) had the resistance value of 0.450 (72.354%). The environmental protection sub-criterion (MO-6) had the resistance value of 0.376 (72.354%). International regulations sub-criterion (MO-7) had the endurance value of 0.364 (70.757%). All maritime operation (MO) sub-criteria fall in the acceptable category, namely level 4, with the exception of the safety sub-criterion, classified as high resilience category - level 5.

Sub-variables	Weight	Score	Result	%	Explanation
Threats	0.248	3.792	0.940	75.836	Acceptable resilience
Vulnerabilities	0.248	3.031	0.751	60.629	Low resilience
Regulations	0.111	2.958	0.327	59.150	Low resilience
Technologies	0.248	3.024	0.749	60.485	Low resilience
Collaboration	0.146	3.080	0.450	61.598	Acceptable resilience
Maritime cybersecurity (MC)	1.000		**3.217**	64.339	Acceptable resilience

Table 11. Evaluated values of maritime cyber resilience for maritime cybersecurity (MC) criteria

The evaluation of maritime cyber resilience in the maritime cybersecurity (MC) criteria consists of five sub-criteria, namely the threats sub-criterion (MC-1) with the resilience value of 0.940 (75.836%). The vulnerabilities sub-criterion (MC-2) has the resilience value of 0.751 (60.629%). The regulations sub-criterion (MC-3) has the endurance value of 0.327 (59.150%). The technologies sub-criterion (MC-4) has the endurance value of 0.749 (60.485%). The collaboration sub-criterion (MC-5) has the endurance value of 0.450 (61.598%). Three sub-criteria are in the Low category at level 3, namely vulnerabilities (MC-2), regulations (MC-3), and technologies (MC-4), while the threats (MC-1) and collaboration (MC-5) sub-criteria are in the Acceptable category at level 4.

Criteria	Result	%	Explanation
Cyber resilience (CR)	3.554	71.074	Acceptable resilience
Maritime operation (MO)	3.834	76.688	Acceptable resilience
Maritime cybersecurity (MC)	3.217	64.339	Acceptable resilience
Resilience result	**3.535**	**70.701**	**Acceptable resilience**

Table 12. Evaluated value of maritime cyber resilience in the Indonesian Sea area

Based on Table 12, the evaluated value of maritime cyber resilience can be concluded to consist of three main criteria. The cyber resilience (CR) criterion has the resilience value of 3554 (71.074%). The maritime operation (MO) criteria have the resilience value of 3834 (76.688%). The maritime cybersecurity (MC) criteria have the resilience value of 3217 (64.339%). Although the maritime operation (MO) criterion has the highest resilience value, overall the evaluated value of maritime cyber resilience falls in the acceptance resilience category level 4, with the value of 3535 (70.701%). In the current maritime operation, there is an increasing dependence on digitalization, integration, automation and network-based systems (Larsen and Lund, 2021). The convergence and digitalization of IT and operational technology (OT) are driving the transformation to the maritime route of operations, which broadens cyber threat scope (Tam et al., 2023).

Information system solutions are increasingly used in the maritime industry, and ultimately all aspects of maritime operations will be assisted by digital transformation (Kechagias et al., 2022). However, while digital technologies offer several advantages for maritime operations, they also leave ships open to cyberattacks (Junior et al., 2021). The history of maritime operations and the effects of being aware of dangers and effects in physical space are extensive (Jones, Tam and Papadaki, 2016). Cyberattacks can cause navigational accidents, pollution, significant financial losses, and even loss of human life in the maritime environment (Junior et al., 2021). Resilient maritime operations are activities at sea that must be carried out by organizations that will not lose control over these activities, capable of enduring and recovering from these activities in the face of challenges (Erstad et al., 2021).

4.4. Maritime cyber resilience model simulation

In this research, the Stella 9 software was used to simulate the dynamic process of maritime cyber resilience with the results shown in Figure 6. Figure 6 shows the dynamic process of maritime cyber resilience in the national sea area. In the 2022-2025 period, maritime cyber resilience is still at level 4 (acceptance resilience); however, this value is dynamic due to dynamic environmental and internal situations with model settings (initial value 0 and maximum 5).

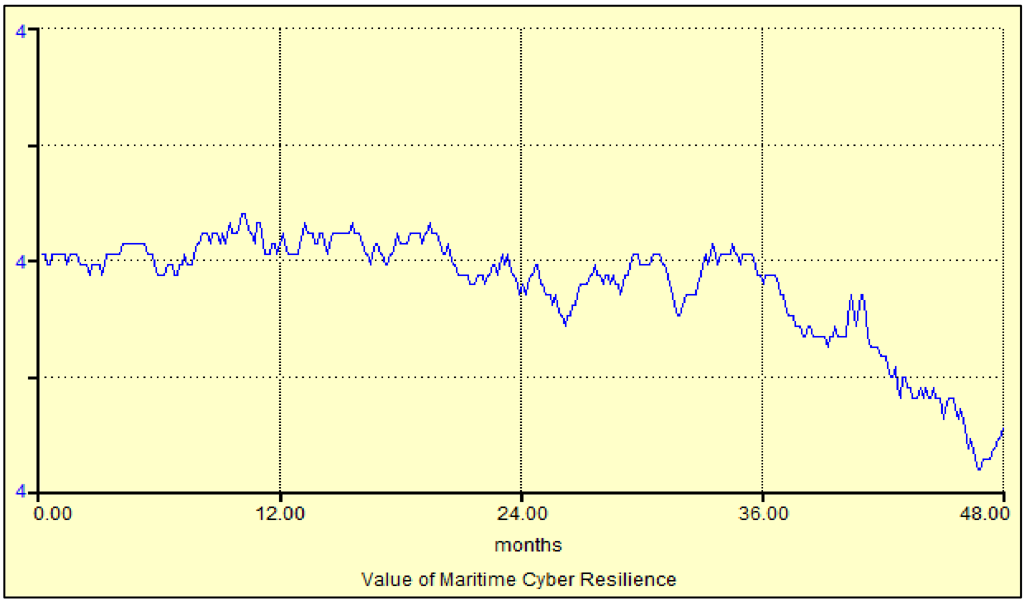

Figure 6. Output value of maritime cyber resilience every year over a 48-month period

Figure 6 also shows that, in the first year of evaluation (in 2022), the developed maritime cyber resilience had a stable value with close to a high score at the end of the year. It is critical to call attention to the underlying assumptions behind this paradigm. The initial assumption was that each maritime cybersecurity stakeholder included in the guidelines was crucial to the exchange of threat data. Some stakeholders might have been left out of the model or others who weren't essential to the modeling process might have been added. This condition is closely related to the fact that stakeholder cybersecurity responsibilities vary throughout the life cycle, from design, commissioning, construction, and operation (Nganga et al., 2022). Additionally, operational aspects of maritime cybersecurity were investigated by looking into its human components (Erstad et al., 2021). The prediction for 2023 is presented in Figure 6 - cyber maritime resilience is expected to be stable, with the development and training carried out in keeping with the trends and situations which are still at level 4. To ensure maritime cyber resilience, human resources were regarded as one of the key assets with a significant role. To develop human resources, many factors must be taken into account, such as the need to include scientific and mental aptitudes in the recruitment process (Permana, 2021). Companies are one type of actor which may have resources that can be allocated to maritime cyber resilience (Hausken, 2020).

In the third and fourth years (2024-2025), a downward trend in the value of maritime cyber resilience is expected. Stakeholders are expected to realize they cannot ignore the deterioration of cyber maritime resilience much longer as a result of the fast-growing number of cyberattacks and new regulatory tools, according to several maritime companies. Given that hackers can determine which stakeholders are least worried about cyber maritime security by learning enough about cargo and routes, there are more frequent and active attacks on the sector (Nganga et al., 2022).

Therefore, the supply chain must be protected by creating a multi-layered cybersecurity system that meets stringent standards, that include ships engaged in sea transportation, and keeping an eye on threats to effectively combat dangers to ships and shipping companies. This system should be developed using a goal-oriented methodology. Technologies that will allow shipowners to take this course and adopt appropriate cyber resilience measures that encompass a variety of aspects, including technology, policy, processes, and personnel, including crew members must be developed (Melnyk et al., 2022).

Furthermore, knowing which technologies and tools to buy, as well as which approach to use, is necessary for resource deployment. The available strategies can be expanded or scaled down depending on the tools and technologies used. Although certain solutions could be costly and improve cyber resilience, they might also have disadvantages or restrictions that could jeopardize maritime cyber resilience. The selection of tools and technologies, as well as upgrading them over time, and adapting to change, has an impact on maritime cyber resilience over time.

4.5. Implications

Research on maritime cyber resilience differs from other cyber research by several criteria and sub-criteria. It is therefore necessary to consider the implications and potential impact of research from a broader perspective. Currently, both the number of studies and the number of researchers working in the field of maritime cybersecurity are relatively lower than is characteristic of many long-established research fields, such as finance, energy, and communications. However, the need for qualified researchers is likely to increase sharply in the future due to the growing digitalization in the maritime industry.

At the same time, efforts to increase awareness of cyber security are becoming increasingly important. The maritime sector lacks a culture of cyber awareness and effective cyber governance, which can reduce its resilience and increase the frequency of cyberattacks. To promote knowledge of cybersecurity in the maritime domain, stakeholders must also create a cybersecurity management system. For all these reasons, the professional responsibility of researchers studying maritime cybersecurity is greater than in any other field. Both the authors and readers of this paper need to be aware of potential implications, as well as of the potential challenges by taking into account several other criteria and sub-criteria. These recommendations show how the practical results of this study, which have broad repercussions and would benefit from further research, particularly in the area of maritime cybersecurity, might be applied. Without question, the rapid technological transformation of the industry will require that the future of maritime cyber resilience stays up to date. Maritime transport is expected to transition from semi-autonomous systems to more autonomous systems and possibly remotely operated unmanned vessels in the future.

5. CONCLUSION

In recent years, the maritime industry has become increasingly dependent on digital technology, making it vulnerable to cyber threats. The consequences of cyberattacks on the maritime industry can be dire, ranging from financial losses to environmental disasters. The purpose of this paper is to provide an evaluation and model simulation of cybersecurity in the maritime domain. It covers the three criteria and eighteen sub-criteria that maritime cyber resilience depends on in the light of the findings. The results of the research with global weight revealed that the threat (MC-1), vulnerability (MC-2), and technologies (MC-3) sub-criteria were considered the most important, with the global weight of 0.102 each, followed by the navigation sub-criteria (MO-2), and governance and compliance (CR-6) with the global weight of 0.072 and 0.065, respectively. The evaluated value of maritime cyber resilience consists of three main criteria. The cyber resilience (CR) criterion has the resilience value of 3554 (71.074%), the maritime operation (MO) criteria have the resilience value of 3834 (76.688%), while the maritime cybersecurity (MC) criteria have the resilience value of 3217 (64.339%). The maritime operation (MO) criterion has the highest resilience value. Overall, the evaluated value of maritime cyber resilience is in the acceptance resilience category level 4, with the value of 3535 (70,701%).

Furthermore, in spite of the change in the value of maritime cyber resilience in the 2022-2025 period, maritime cyber resilience is still at level 4 (acceptance resilience). Predictions for 2023 are that maritime cyber resilience will tend to be stable and remain at level 4. In the third and fourth years (2024-2025), a downward trend in the value of maritime cyber resilience is anticipated. As a result, it is essential to create a multi-layered cybersecurity system that meets the high standards to safeguard the supply chain, that will include ships engaged in sea transportation, and staying up to date with the risks to effectively counter threats to the maritime industry and shipping companies.

Limitations & future research

In this study, maritime cyber resilience was evaluated by looking at the relevant criteria determined and by weighting the important sub-criteria. By concentrating on issues related to maritime resilience and establishing strategic initiatives, managing maritime cyber resilience will move on to the next stage. This serves as a foundation for the creation of new decision-making techniques that will facilitate the implementation of sustainability strategies or the identification of risk-based security measures in the most effective way possible. Second, the main limitation is the number of participants. Additionally, hearing opinions from those who assert to be experts in the maritime and cyber domains is helpful. A quantitative method in future work could bring this poll to a larger audience.

Another limitation of this study is that the accuracy of the measurement depends on the selection of maritime cyber resilience criteria and sub-criteria that make up the resilience matrix (RM), as well as on the level of reliability and trustworthiness of an organization's data, which can be interpreted as organizational bias and may affect accuracy. In the future, algorithms and data structures may be improved to enhance data collection methods and reduce bias. Likewise, this study did not take into account cyberattack scenarios and provided modeling faced with resilience dynamics. Therefore, additional research is required to take into account attacks, multiple attackers with different targets, and various attack scenarios that are not described in this paper. Future research should also take into account more network-level protection tactics.

ACKNOWLEDGMENT

This study was supported by the Indonesian Defense University, the Airlangga University, and the Indonesian Naval Technology College.

CONFLICT OF INTEREST

The authors declared no potential conflicts of interest with respect to the research, authorship and publication of this article.

REFERENCES

Afenyo, M. and Caesar, L. D. 2023 ‘Maritime cybersecurity threats: Gaps and directions for future research’, Ocean and Coastal Management, 236, p. 106493. Available at: https://dx.doi.org/10.1016/j.ocecoaman.2023.106493.

Akpan, F. et al. 2022 ‘Cybersecurity Challenges in the Maritime Sector’, Network, 2(1), pp. 123–138. Available at: https://dx.doi.org/10.3390/network2010009.

Aksha, S. K. et al. 2019 ‘An Analysis of Social Vulnerability to Natural Hazards in Nepal Using a Modified Social Vulnerability Index’, International Journal of Disaster Risk Science, 10(1), pp. 103–116. Available at: https://dx.doi.org/10.1007/s13753-018-0192-7.

Aljuhami, A. M. and Bamasoud, D. M. 2021 ‘Cyber Threat Intelligence in Risk Management’, International Journal of Advanced Computer Science and Applications, 12(10), pp. 156–164. Available at: https://dx.doi.org/10.14569/ijacsa.2021.0121018.

Almanasreh, E., Moles, R. and Chen, T. F. 2019 ‘Evaluation of methods used for estimating content validity’, Research in Social and Administrative Pharmacy, 15(2), pp. 214–221. Available at: https://dx.doi.org/10.1016/j.sapharm.2018.03.066.

Androjna, A. and Perkovič, M. 2021 ‘Impact of spoofing of navigation systems on maritime situational awareness’, Transactions on Maritime Science, 10(2), pp. 361–373. Available at: https://dx.doi.org/10.7225/toms.v10.n02.w08.

Arora, A. et al. 2020 ‘Identifying sustainability drivers in higher education through fuzzy AHP’, Higher Education, Skills and Work-based Learning, 11(4), pp. 823–836. Available at: https://dx.doi.org/10.1108/HESWBL-03-2020-0051.

Boyes, H. A. 2014 ‘Maritime Cyber Security – Securing the Digital Seaways’, Engineering & Technology Reference, January. Available at: https://dx.doi.org/10.1049/etr.2014.0009.

Bueger, C. 2015 ‘What is maritime security?’, Marine Policy, 53, pp. 159–164. Available at: https://dx.doi.org/10.1016/j.marpol.2014.12.005.

Caprolu, M. et al. 2020 ‘Vessels Cybersecurity: Issues, Challenges, and the Road Ahead’, IEEE Communications Magazine, 58(6), pp. 90–96. Available at: https://dx.doi.org/10.1109/MCOM.001.1900632.

Carías, J. F. et al. 2019 ‘The dynamics of cyber resilience management’, Proceedings of the International ISCRAM Conference, 2019-May, pp. 64–75.

Carías, J. F. et al. 2020 ‘Systematic approach to cyber resilience operationalization in SMEs’, IEEE Access, 8, pp. 174200–174221. Available at: https://dx.doi.org/10.1109/ACCESS.2020.3026063.

Ding, J. et al. 2022 ‘Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions’, Energies, 15(18), pp. 1–37. Available at: https://dx.doi.org/10.3390/en15186799.

Dolezal, O. and Tomaskova, H. 2018 ‘Czech cyber security system from a view of system dynamics’, Journal of Cyber Security and Mobility, 8(2), pp. 241–260. Available at: https://dx.doi.org/10.13052/jcsm2245-1439.824.

Drazovich, L., Brew, L. and Wetzel, S. 2021 ‘Advancing the state of maritime cybersecurity guidelines to improve the resilience of the maritime transportation system’, Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, CSR 2021, pp. 503–509. Available at: https://dx.doi.org/10.1109/CSR51186.2021.9527922.

Enoch, S. Y., Lee, J. S. and Kim, D. S. 2021 ‘Novel security models, metrics and security assessment for maritime vessel networks’, Computer Networks, 189, p. 107934. Available at: https://dx.doi.org/10.1016/j.comnet.2021.107934.

Erstad, E. et al. 2023 ‘A human-centred design approach for the development and conducting of maritime cyber resilience training’, WMU Journal of Maritime Affairs, (0123456789). Available at: https://dx.doi.org/10.1007/s13437-023-00304-7.

Erstad, E., Ostnes, R. and Lund, M. S. 2021 ‘An operational approach to maritime cyber resilience’, TransNav, 15(1), pp. 27–34. Available at: https://dx.doi.org/10.12716/1001.15.01.01.

Fallah, M. and Ocampo, L. 2021 ‘The use of the Delphi method with non-parametric analysis for identifying sustainability criteria and indicators in evaluating ecotourism management: the case of Penang National Park (Malaysia)’, Environment Systems and Decisions, 41(1), pp. 45–62. Available at: https://dx.doi.org/10.1007/s10669-020-09790-z.

Freire, W. P. et al. 2022 ‘Towards a Secure and Scalable Maritime Monitoring System Using Blockchain and Low-Cost IoT Technology’, Sensors, 22(13), pp. 1–20. Available at: https://dx.doi.org/10.3390/s22134895.

Ghelani, D. 2022 ‘Cyber security, cyber threats, implications and future perspectives: A Review’, American Journal of Science, Engineering and Technology, 3(6), pp. 12–19. Available at: https://dx.doi.org/10.11648/j.XXXX.2022XXXX.XX.

Greiman, V. 2020 ‘Defending the Cyber Sea: Legal Challenges Ahead - ProQuest’, Journal of Information Warfare, 19(3), pp. 68–82. Available at: https://www.proquest.com/docview/2435722737/A48026DE74D94390PQ/3?accountid=10286.

Gu, J. and Liu, Z. 2022 ‘TOPSIS-Based Algorithm for Resilience Indices Construction and the Evaluation of an Electrical Power Transmission Network’, Symmetry, 14(5). Available at: https://dx.doi.org/10.3390/sym14050985.

Gunes, B., Kayisoglu, G. and Bolat, P. 2021 ‘Cyber security risk assessment for seaports: A case study of a container port’, Computers and Security, 103. Available at: https://dx.doi.org/10.1016/j.cose.2021.102196.

Hanson, W. E. et al. 2005 ‘Mixed methods research designs in counseling psychology’, Journal of Counseling Psychology, 52(2), pp. 224–235. Available at: https://dx.doi.org/10.1037/0022-0167.52.2.224.

Hareide, O. S. et al. 2018 ‘Enhancing Navigator Competence by Demonstrating Maritime Cyber Security’, Journal of Navigation, 71(5), pp. 1025–1039. Available at: https://dx.doi.org/10.1017/S0373463318000164.

Hausken, K. 2020 ‘Cyber resilience in firms, organizations and societies’, Internet of Things (Netherlands), 11, pp. 1–9. Available at: https://dx.doi.org/10.1016/j.iot.2020.100204.

Herrera, H. 2017 ‘From Metaphor to Practice: Operationalizing the Analysis of Resilience Using System Dynamics Modelling’, Systems Research and Behavioral Science, 34(4), pp. 444–462. Available at: https://dx.doi.org/10.1002/sres.2468.

Hult Khazaie, D. and Khan, S. S. 2020 ‘Social psychology and pandemics: Exploring consensus about research priorities and strategies using the Delphi method’, Asian Journal of Social Psychology, 23(4), pp. 363–371. Available at: https://dx.doi.org/10.1111/ajsp.12442.

Humayun, M. et al. 2020 ‘Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study’, Arabian Journal for Science and Engineering, 45(4), pp. 3171–3189. Available at: https://dx.doi.org/10.1007/s13369-019-04319-2.

Improta, G. et al. 2018 ‘Use of the AHP methodology in system dynamics: Modelling and simulation for health technology assessments to determine the correct prosthesis choice for hernia diseases’, Mathematical Biosciences, 299, pp. 19–27. Available at: https://dx.doi.org/10.1016/j.mbs.2018.03.004.

Jacq, O. et al. 2019 ‘Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre’, 2018 2nd Cyber Security in Networking Conference, CSNet 2018. Available at: https://dx.doi.org/10.1109/CSNET.2018.8602669.

Jones, K. D., Tam, K. and Papadaki, M. 2016 ‘Threats and Impacts in Maritime Cyber Security’, Engineering & Technology Reference, pp. 1–12. Available at: https://dx.doi.org/10.1049/etr.2015.0123.Published.

Jovanović, A. et al. 2020 Assessing resilience of healthcare infrastructure exposed to COVID-19: emerging risks, resilience indicators, interdependencies and international standards, Environment Systems and Decisions. Springer US. Available at: https://dx.doi.org/10.1007/s10669-020-09779-8.

Kanwal, K. et al. 2022 ‘Maritime cybersecurity: are onboard systems ready?’, Maritime Policy and Management, 00(00), pp. 1–19. Available at: https://dx.doi.org/10.1080/03088839.2022.2124464.

Kapalidis, C. et al. 2022 ‘A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships’, Journal of Marine Science and Engineering, 10(10). Available at: https://dx.doi.org/10.3390/jmse10101486.

Karamperidis, S., Kapalidis, C. and Watson, T. 2021 ‘Maritime cyber security: A global challenge tackled through distinct regional approaches’, Journal of Marine Science and Engineering, 9(12). Available at: https://dx.doi.org/10.3390/jmse9121323.

Kechagias, E. P. et al. 2022 ‘Digital transformation of the maritime industry: A cybersecurity systemic approach’, International Journal of Critical Infrastructure Protection, 37, p. 100526. Available at: https://dx.doi.org/10.1016/j.ijcip.2022.100526.

Khalid Khan, S., Shiwakoti, N. and Stasinopoulos, P. 2022 ‘A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles’, Accident Analysis and Prevention, 165. Available at: https://dx.doi.org/10.1016/j.aap.2021.106515.

Khalilzadeh, M., Katoueizadeh, L. and Zavadskas, E. K. 2020 ‘Risk identification and prioritization in banking projects of payment service provider companies: an empirical study’, Frontiers of Business Research in China, 14(1). Available at: https://dx.doi.org/10.1186/s11782-020-00083-5.

Kim, K. and Kim, B. 2022 ‘Decision-Making Model for Reinforcing Digital Transformation Strategies Based on Artificial Intelligence Technology’, Information (Switzerland), 13(5). Available at: https://dx.doi.org/10.3390/info13050253.

Kolini, F. and Janczewski, L. 2015 ‘Cyber Defense Capability Model: A Foundation Taxonomy’, International Conference on Information Resources Management (CONF-IRM). Available at: http://aisel.aisnet.org/confirm2015/32.

Kotis, K., Stavrinos, S. and Kalloniatis, C. 2023 ‘Review on Semantic Modeling and Simulation of Cybersecurity and Interoperability on the Internet of Underwater Things’, Future Internet, 15(1). Available at: https://dx.doi.org/10.3390/fi15010011.

Kulugh, V. E., Mbanaso, U. M. and Chukwudebe, G. 2022 ‘Cybersecurity Resilience Maturity Assessment Model for Critical National Information Infrastructure’, SN Computer Science, 3(3), pp. 1–15. Available at: https://dx.doi.org/10.1007/s42979-022-01108-x.

Larsen, M. H. and Lund, M. S. 2021 ‘Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review’, IEEE Access, 9, pp. 144895–144905. Available at: https://dx.doi.org/10.1109/ACCESS.2021.3122433.

Lee, S., Huh, J.-H. and Kim, Y. 2020 ‘Python tensorflow big data analysis for the security of korean nuclear power plants’, Electronics (Switzerland), 9(9), pp. 1–19. Available at: https://dx.doi.org/10.3390/electronics9091467.

Leite Junior, W. C. et al. 2021 ‘A triggering mechanism for cyber-attacks in naval sensors and systems’, Sensors, 21(9), pp. 1–22. Available at: https://dx.doi.org/10.3390/s21093195.

Li, G. et al. 2020 ‘System dynamics modelling for improving urban resilience in Beijing, China’, Resources, Conservation and Recycling, 161, p. 104954. Available at: https://dx.doi.org/10.1016/j.resconrec.2020.104954.

Malatji, M., Marnewick, A. L. and Von Solms, S. 2022 ‘Cybersecurity capabilities for critical infrastructure resilience’, Information and Computer Security, 30(2), pp. 255–279. Available at: https://dx.doi.org/10.1108/ICS-06-2021-0091.

Maletič, D. et al. 2021 ‘Framework development of an asset manager selection based on risk management and performance improvement competences’, Safety, 7(1). Available at: https://dx.doi.org/10.3390/safety7010010.

Mbanaso, U. M., Lucienne Abrahams and Apene, O. Z. 2019 ‘Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework’, The African Journal of Information and Communication (AJIC), (23), pp. 1–26. Available at: https://dx.doi.org/10.23962/10539/27535.

McGillivary, P. 2018 ‘Why maritime cybersecurity is an ocean policy priority and how it can be addressed’, Marine Technology Society Journal, 52(5), pp. 44–57. Available at: https://dx.doi.org/10.4031/MTSJ.52.5.11.

Melnyk, O. et al. 2022 ‘Review of Ship Information Security Risks and Safety of Maritime Transportation Issues’, TransNav, 16(4), pp. 717–722. Available at: https://dx.doi.org/10.12716/1001.16.04.13.

Mraković, I. and Vojinović, R. 2019 ‘Maritime cyber security analysis – How to reduce threats?’, Transactions on Maritime Science, 8(1), pp. 132–139. Available at: https://dx.doi.org/10.7225/toms.v08.n01.013.

Mustajoki, J. et al. 2020 ‘Utilizing ecosystem service classifications in multi-criteria decision analysis – Experiences of peat extraction case in Finland’, Ecosystem Services, 41, p. 101049. Available at: https://dx.doi.org/10.1016/j.ecoser.2019.101049.

Nganga, A. et al. 2022 ‘Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment’, in The Seventh International Conference on Cyber-Technologies and Cyber-Systems.

Noor, M. M. 2022 ‘Addressing cyber security vulnerabilities and initiatives in Malaysia maritime industry’, Journal of Maritime Research, 19(3), pp. 89–95. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85144189714&partnerID=40&md5=e37a6a47013e55b704eb6b5789595f7d.

Octavian, A. et al. 2021 ‘Combined multi-criteria decision making and system dynamics simulation of social vulnerability in southeast Asia’, Decision Science Letters, 10(3), pp. 323–336. Available at: https://dx.doi.org/10.5267/j.dsl.2021.2.005.

Oruc, A. 2022 'Ethical Considerations in Maritime Cybersecurity Research', TransNav, 16(2), pp. 309–318. Available at: https://dx.doi.org/10.12716/1001.16.02.14.

Park, C. et al. 2019 'Cybersecurity in the maritime industry: A literature review', 20th Commemorative Annual General Assembly, AGA 2019 - Proceedings of the International Association of Maritime Universities Conference, IAMUC 2019, pp. 79–86.

Park, C. et al. 2023 'A BN driven FMEA approach to assess maritime cybersecurity risks', Ocean and Coastal Management, 235(November 2022), p. 106480. Available at: https://doi.org/10.1016/j.ocecoaman.2023.106480.

Permana, A. 2021 'Indonesia's Cyber Defense Strategy in Mitigating the Risk of Cyber Warfare Threats', Syntax Idea, 3(1), pp. 1–11.

Peter, A. S. 2017 'Cyber resilience preparedness of Africa's top-12 emerging economies', International Journal of Critical Infrastructure Protection, 17, pp. 49–59. Available at: https://doi.org/10.1016/j.ijcip.2017.03.002.

Progoulakis, I. et al. 2021 'Perspectives on cyber security for offshore oil and gas assets', Journal of Marine Science and Engineering, 9(2), pp. 1–27. Available at: https://doi.org/10.3390/jmse9020112.

Raicu, A. and Raicu, G. 2021 'Digital Enterprise and Cyber Security Evolution', Macromolecular Symposia, 396(1). Available at: https://doi.org/10.1002/masy.202000326.

Razikin, K. and Soewito, B. 2022 'Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework', Egyptian Informatics Journal, 23(3), pp. 383–404. Available at: https://doi.org/10.1016/j.eij.2022.03.001.

Rehak, D. et al. 2019 'Complex approach to assessing resilience of critical infrastructure elements', International Journal of Critical Infrastructure Protection, 25, pp. 125–138. Available at: https://doi.org/10.1016/j.ijcip.2019.03.003.

Rioja-Lang, F. C. et al. 2020 'Determining a welfare prioritization for horses using a Delphi method', Animals, 10(4), pp. 1–16. Available at: https://doi.org/10.3390/ani10040647.

Rios Insua, D. et al. 2021 'An Adversarial Risk Analysis Framework for Cybersecurity', Risk Analysis, 41(1), pp. 16–36. Available at: https://doi.org/10.1111/risa.13331.

Roege, P. E. et al. 2017 Bridging the gap from cyber security to resilience, NATO Science for Peace and Security Series C: Environmental Security. Available at: https://doi.org/10.1007/978-94-024-1123-2_14.

Seetharaman, A. et al. 2021 'Impact of Factors Influencing Cyber Threats on Autonomous Vehicles', Applied Artificial Intelligence, 35(2), pp. 105–132. Available at: https://doi.org/10.1080/08839514.2020.1799149.

Sepúlveda Estay, D. A. 2021 'A system dynamics, epidemiological approach for high-level cyber-resilience to zero-day vulnerabilities', Journal of Simulation, 00(00), pp. 1–16. Available at: https://doi.org/10.1080/17477778.2021.1890533.

Shahzad, M., Awan, K. and Ghamdi, M. A. Al 2019 'Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS)', Journal of Marine Science and Engineering, 7(350), pp. 1–20. Available at: https://doi.org/10.3390/jmse7100350.

Sharma, Vikrant et al. 2019 'Implementation model for cellular manufacturing system using AHP and ANP approach', Benchmarking, 26(5), pp. 1605–1630. Available at: https://doi.org/10.1108/BIJ-08-2018-0253.

Steingartner, W., Galinec, D. and Kozina, A. 2021 'Threat defense: Cyber deception approach and education for resilience in hybrid threats model', Symmetry, 13(4), pp. 1–25. Available at: https://doi.org/10.3390/sym13040597.

Susilo, A. K. et al. 2019 'Navy development strategy to encounter threat of national maritime security using SWOT-fuzzy multi criteria decision making (F-MCDM)', Journal of Maritime Research, 16(1), pp. 3–16.

Taguchi, N. 2018 'Description and explanation of pragmatic development: Quantitative, qualitative, and mixed methods research', System, 75, pp. 23–32. Available at: https://doi.org/10.1016/j.system.2018.03.010.

Tam, K. and Jones, K. D. 2018 'Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping', Journal of Cyber Policy, 3(2), pp. 147–164. Available at: https://doi.org/10.1080/23738871.2018.1513053.

Tam, K. et al. 2023 'Quantifying the econometric loss of a cyber-physical attack on a seaport', Frontiers in Computer Science, 4. Available at: https://doi.org/10.3389/fcomp.2022.1057507.

Tweneboah-Koduah, S., Skouby, K. E. and Tadayoni, R. 2017 ‘Cyber Security Threats to IoT Applications and Service Domains’, Wireless Personal Communications, 95(1), pp. 169–185. Available at: https://doi.org/10.1007/s11277-017-4434-6.

Wahl, A. M. 2020 ‘Expanding the concept of simulator fidelity: the use of technology and collaborative activities in training maritime officers’, Cognition, Technology and Work, 22(1), pp. 209–222. Available at: https://doi.org/10.1007/s10111-019-00549-4.

Yaacoub, J.-P. A. et al. 2022 ‘Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations’, International Journal of Information Security, 21(1), pp. 115–158. Available at: https://doi.org/10.1007/s10207-021-00545-8.