JOURNAL OF MARITIME RESEARCH

Vol XXI. No. II (2024) pp 171–180

ISSN: 1697-4840, www.jmr.unican.es

Key Factors of Cyber Resilience in Maritime Domain using Analytical Hierarchy Process (AHP)

Yoyok Nurkarya Santosa[1,*], Dhiana Puspitawati[1], I Nengah Putra[2], A.K. Susilo[3], A.R. Prabowo[3]

ARTICLE INFO

Article history:
Received 20 Dec 2023;
in revised from 18 Jan 2024;
accepted 29 Mar 2024.

Keywords:
Maritime Cyber Resilience; Analytical Hierarchy Process (AHP); Cyber Security; Maritime Operation.

ABSTRACT

In recent years, the maritime industry has become increasingly dependent on digital technology, making it vulnerable to cyber threats. One of the main challenges in achieving maritime cyber resilience is the complexity of the maritime ecosystem. It should also include a resiliency brief that addresses cyber intrusion response and recovery plans, as well as recommendations for systems that improve cyber resilience. This research aims to identify and assess key cyber resilience factors in the maritime domain. This research uses a descriptive statistical qualitative method approach supported by the Analytical Hierarchy Process (AHP) with the Indonesian maritime shipping industry as the research locus domain and expert panel of eight personnel (academicians and practitioners). The Indonesian sea area is the locus of research. The results of 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 a global weight of 0.102 each followed by the Navigation sub-criteria (MO-2). and Governance and Compliance (CR-6) with a global weight of 0.072 and 0.065 respectively.

1. Introduction.

In recent years, the maritime industry has increasingly relied on digital technology, making it vulnerable to cyber threats (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 government agencies (Park et al., 2019). Each stakeholder has risks and challenges to cyber security that must be overcome (Drazovich, Brew and Wetzel, 2021).

The An emerging approach to tackling this problem is cyber resilience. This approach is generally defined as the ability to anticipate, detect, contain, develop, and recover after a cyber incident, from an organizational, technological, and human perspective (Carías et al., 2020). Sharing information about cyber incidents provides benefits for raising awareness, reducing vulnerability, managing risk, and increasing cyber resilience (Oruc, 2022). It should also include a strategy for resilience 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), explaining the need for future research in implementing cyber security capability frameworks, 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 exploration through dynamic models to be able to consider different levels and network hierarchies in cyber-resilience. According to Park et al. (2023), further research is needed from an evaluation perspective for cyber security and resilience (Hausken, 2020) in the maritime industry in mitigating cyber threats (Afenyo and Caesar, 2023). Therefore, it is necessary to identify key factors of cyber resilience in the maritime domain.

[1] Brawijaya University, Ketawanggede, Lowokwaru, Malang, Indonesia.

[2] Indonesia Defense University, Citeureup-Bogor, Indonesia.

[3] Indonesia Navy Technology College (STTAL), Bumi Moro, Morokrembangan, Surabaya, Indonesia.

[*] Corresponding author: Yoyok Nurkarya Santosa. E-mail Address: ynksantosa@student.ub.ac.id.

This study aims to provide an assessment and model simulation of cyber security in the maritime domain. This study uses a qualitative descriptive statistical method approach. This research is also supported by Analytical Hierarchy Process (AHP) with an expert panel of eight personnel (academicians and practitioners) and the research period is January 2023 – September 2023. The Indonesian maritime area is the locus of research because it is a cross-economic pathway world maritime (Susilo et al., 2019).

This research is important in helping to identify 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 strategies to mitigate risks. Assessing cyber resilience helps stakeholders comply with this guidance and other relevant regulations. By demonstrating a commitment to cyber security and resilience, stakeholders can build trust among themselves and with customers who rely on maritime services.

2. Literature Review.

2.1. Cyber resilience.

Cyber resilience refers to the evolving capabilities to resist cyber attacks and mitigate risks. Individual and interconnected economies need to maximize the value attached to 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 cyber attacks (Carías et al., 2019). Cyber resilience recognizes that cyber-attacks are unavoidable and that organizations need to be prepared to respond quickly and effectively when they occur (Erstad et al., 2023).

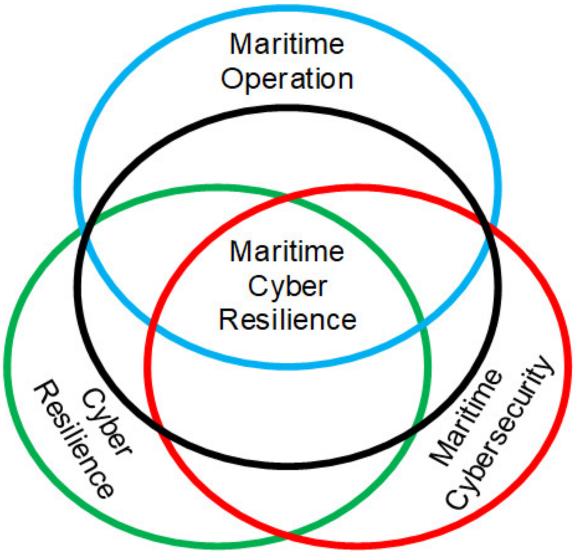
There are several key components of cyber resilience (Drazovich, Brew and Wetzel, 2021). First, organizations need to have a comprehensive understanding of IT infrastructure and the potential risks it faces (Hausken, 2020). Second, organizations need to have an effective incident response plan (Steingartner, 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).

2.2. Maritime Cyber Resilience.

Digital competency, Maritime operations are activities at sea that must be carried out by organizations so they do not lose control over these activities and can continue and recover these activities in the face of challenges (Erstad et al., 2021). Maritime Cyber Resilience started as a component of maritime cyber risk management. Maritime cyber risk management is an interdisciplinary subject, consisting of aspects such as resilience, safety, and maritime cybersecurity, so students need to develop skills to work together and respond collaboratively (Erstad et al., 2023). As maritime cyber security emphasizes the ability to anticipate, contain, recover from, and evolve from cyber threats in minimum time (Erstad et al., 2021), it serves as a unifying concept, contributing to maritime cyber risk management knowledge.

Maritime Cyber Resilience has been defined as the ability of maritime systems to learn how to maintain and develop normal operations, as well as anticipate, contain, recover and evolve from cyber threats in the shortest possible time (Erstad et al., 2021). According to Erstad et al. (2021), the authors also argue why navigators should be the focus of study when considering maritime cyber resilience, because navigators are on the cutting edge of operations, perhaps being the only agents capable of detecting undesired variations in situations. Furthermore, the navigator is expected to take the helm when technology fails. One of the assumptions when considering maritime cyber resilience is that navigators must accept that the security of the situation can be controlled, and will ultimately be properly controlled.

Figure 1: Origins of Maritime Cyber Resilience.



Source: Authors, adapted from Erstad et al. (2021).

3. Methodology.

This study uses a qualitative descriptive statistical approach. A qualitative design of descriptive statistics at different times and sequentially was initiated by qualitative research beforehand which was supported by data in the form of statistical figures (Hanson et al., 2005; Taguchi, 2018). Data collection in this article is divided into two categories, namely primary data and secondary data. Primary data and as an expert, namely: cyber experts from practitioners and academics. The expert criteria have been determined, namely: 1) From academics with a minimum master's education (Hult Khazaie and Khan, 2020;

Rioja-Lang et al., 2020); 2) From practitioners related (Fallah and Ocampo, 2021) to maritime cyber resilience; 3) Working period of more than 5 years (Khalilzadeh, Katoueizadeh and Zavadskas, 2020; Kim and Kim, 2022); 4) 5 expert judgments (4 doctors, 1 doctoral student) as article Almanasreh et al. (2019). Secondary data: news and information in print media, findings from previous research on online media, archives, regulations and policies, official institutional documents, and official social media accounts.

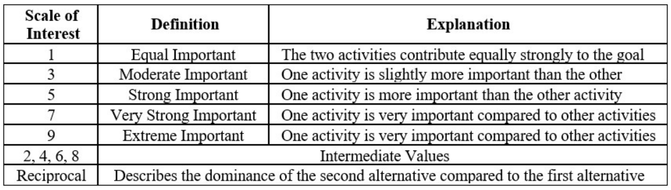
This research will be conducted in Jakarta and several international port areas in Indonesia which represent maritime cyber resilience. This research was conducted from January 2023 – September 2023 by giving a questionnaire to experts based on some secondary data. Nevertheless, observations related 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 makes it vulnerable to cyber attacks in the maritime aspect with Indonesia's vast territory and strategic position in the world is a serious study. Therefore, researchers still see that there are great opportunities or opportunities to be able to enter and make theoretical contributions.

3.1. Analytical Hierarchy Process (AHP).

AHP describes complex multi-factor or multi-criteria problems into a hierarchy, according to Saaty, a hierarchy is defined as a representation of a complex problem in a multi-level structure, where the first level is the objective, followed by the factor, criteria, sub-criteria levels, and so on down to the next level. the last of the alternatives with a hierarchy of a complex problem can be described in groups which are then arranged into a hierarchy as the problem will appear more systematically structured (Saaty, 2006). One of AHP's distinctive advantages, setting it apart from other decision-making models, is its flexibility regarding absolute consistency requirements. This means that while problems can be perceived and assessed, the method does not require complete numerical data for quantitative problem modeling (Siekelova, Podhorska and Imppola, 2021).

Humans can instinctively estimate simple quantities by comparing two objects. For this reason, Saaty established a quantitative scale of 1 to 9 to assess the comparative importance of other elements. There are 7 pillars of AHP modeling, including (Saaty, 2012; Marzouk and Sabbah, 2021): The ratio scale is a comparison of two values (a/b) where the values a and b are of the same type (units); 2) Pairwise comparison; 3) Eigenvector sensitivity conditions; 4) Homogeneity and grouping; 5) Synthesis; 6) Maintaining and reversing the order of weight and order in the hierarchy; 7) Group considerations.

Table 1: AHP Rating Scale.



Scale of Interest	Definition	Explanation
1	Equal Important	The two activities contribute equally strongly to the goal
3	Moderate Important	One activity is slightly more important than the other
5	Strong Important	One activity is more important than the other activity
7	Very Strong Important	One activity is very important compared to other activities
9	Extreme Important	One activity is very important compared to other activities
2, 4, 6, 8	Intermediate Values	
Reciprocal	Describes the dominance of the second alternative compared to the first alternative	

Source: Authors.

The steps of the AHP method include:

1. Creating a pairwise comparison matrix.

$$A = a_{im} = \begin{bmatrix} 1 & a_{12} & \dots & a_{1n} \\ \frac{1}{a_{12}} & 1 & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ \frac{1}{a_{1n}} & \frac{1}{a_{2n}} & \dots & 1 \end{bmatrix} \tag{1}$$

i, m = 1, 2, ... , n = related criteria index.

2. Creating a matrix value criteria.
3. Creating an additional Matrix for Each Row.
4. Assessing Consistency Index (CI) and Consistency Ratio (CR).

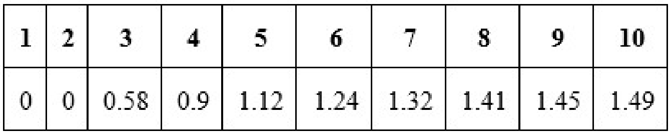
$$CI = \frac{\lambda maks - n}{n}; \tag{2}$$

$$CR = \frac{CI}{RI}; \tag{3}$$

N = Number of Elements,
RI = Random Consistency Index.

If the CR (Consistency Ratio) is 0.1 (i.e., 10%), the matrix is considered consistent, and the decision is accepted. Conversely, if CR is greater than that, it means there are too many contradictions in the matrix. Anticipating the latter situation involves reviewing the matrix and then revising the weights loaded by the vector.

Table 2: Random Consistency Index Value.



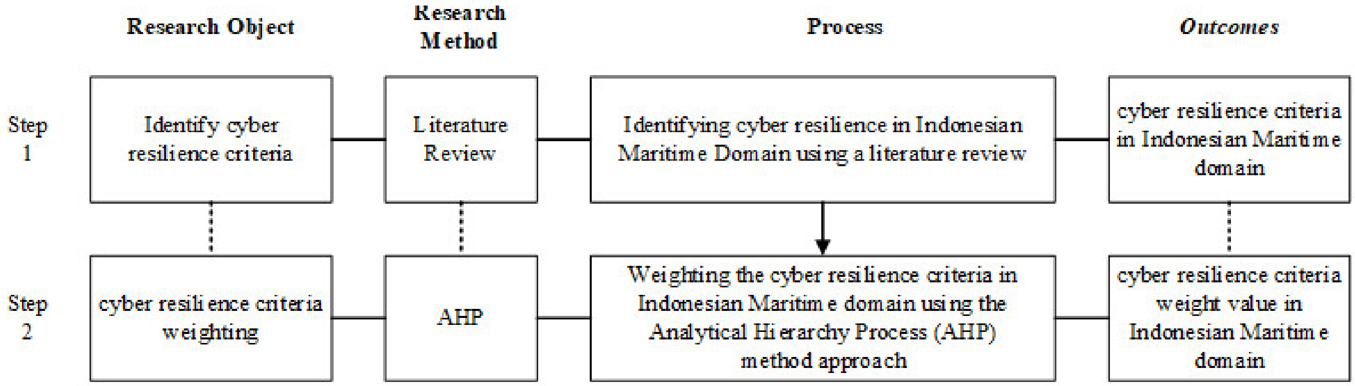
1	2	3	4	5	6	7	8	9	10
0	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.49

Source: Authors.

3.2. Research Design.

The study presented here specifically discusses the resilience of the maritime cyber domain located in the Indonesian sea area which is divided into three stages. First, it uses the approach of previous manuscript literature, brainstorming with questionnaires, and is supported by expert assessments to identify key variables and analyze the values between variables in maritime cyber resilience. Second, the measurement uses the weighting and assessment of maritime cyber resilience. The weighting uses the AHP method with data obtained from selected experts from relevant stakeholders. These experts have been asked to allocate 100% total weight among the variables and sub-variables.

Figure 2: Research design for cyber resilience in Indonesia Maritime domain.


Research Object
Research Method
Process
Outcomes
Step 1
Identify cyber resilience criteria
Literature Review
Identifying cyber resilience in Indonesian Maritime Domain using a literature review
cyber resilience criteria in Indonesian Maritime domain
Step 2
cyber resilience criteria weighting
AHP
Weighting the cyber resilience criteria in Indonesian Maritime domain using the Analytical Hierarchy Process (AHP) method approach
cyber resilience criteria weight value in Indonesian Maritime domain

Source: Authors.

Table 3: Selected Variables for maritime cyber resilience.

Variables	Sub-variables	Coding	References
Cyber Resilience (CR)	Threat Intelligence	CR-1	(Jacq *et al.*, 2019; Mbanaso, Lucienne 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, Lucienne 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)

Source: Authors.

4. Results and Discussion.

4.1. Identification of key variables in maritime cyber resilience.

Identifying key variables is an important step in conducting research or analysis. Key variables are factors that have a significant impact on Maritime cyber resilience. These variables can be identified through reviewing existing literature, consulting with experts in the field, or through exploratory research. Key variables are variables that have a significant impact on research results and are very 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. To enhance maritime cyber resilience, it is important to identify the key variables that impact resilience. When choosing the variables as indicators, this article considers the context and framework set by the main objective of the study, which is to be able to identify areas of maritime cyber security, some modifications have to be made to suit this context. Therefore, the variables that exist in the context of resilience in general have not been considered representative but have been removed or replaced with other variables that are more relevant. The approach here is to use expert judgment as a tool for broad validation of the empirical determination of the indicators described above. Each expert was asked to define his field of expertise in terms of cyber-maritime resilience in the Indonesian Sea region. Some of the identified indicators have been verified by experts (Table 3).

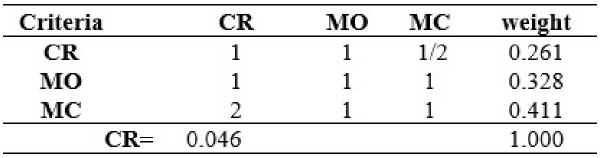
4.2. Weighting of Variable and Sub-variable.

At this stage, each expert is asked to consider the key indicators that are considered the most important in terms of defining or predicting maritime cyber resilience, and then rating the different indicators according to their importance, based on their experience in various areas of cyber maritime resilience assessment. Experts are allowed to perform several different ranking exercises. Experts were also asked to consider whether they felt a distinction could be made between the key indicators representing cyber maritime. Weighting is carried out using the Analytical Hierarchy Process (AHP) method which has a time scale according to the criteria for the relationship between variables and sub-variables.

The output of this model will differ based on the problem examined and will be a vector containing the local weights of the alternatives considered for each sub-criteria. The local vectors that contain the weights of these subcriteria are then normalized and multiplied by the global vectors that contain the weights for the higher-level criteria (parent criteria). This will lead to the final vector of decision problems as in research by Improta et al., (2018). To summarize, each criterion in the hierarchy will be simulated, taking into account not only all the interdependencies between the sub-criteria associated with the same parent criterion but also their variability over time as in system dynamics modeling.

Finally, based on the weight of the scenario rating criteria can be determined, so that certain decision vectors can be obtained at each time step of the simulation process. In this way, the static behavior of conventional AHP approaches can be overcome and time-varying decision-making processes can be implemented. The AHP formula is applied to each criterion and sub-criteria and compared with the simulation results from the model. As a result of the decision-making process, evaluation values and scenarios i.e. the best combination of parameters can be selected. The results of the weighting can be seen in Figure 3 and Table 7.

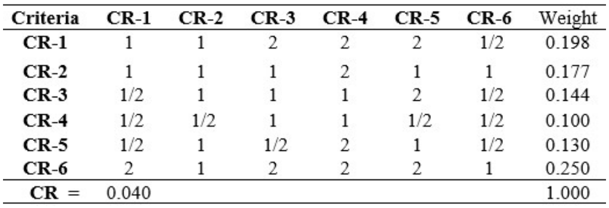
Table 4: Pairwise comparison matrix aggregation for Maritime Cyber Resilience.



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

Source: Authors.

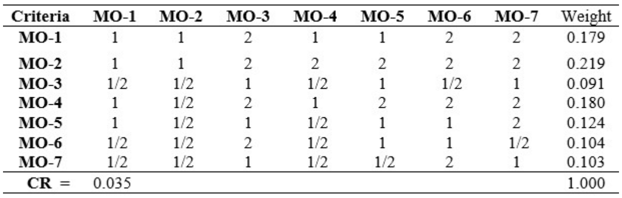
Table 5: Pairwise comparison matrix aggregation for Cyber Resilience variable.



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

Source: Authors.

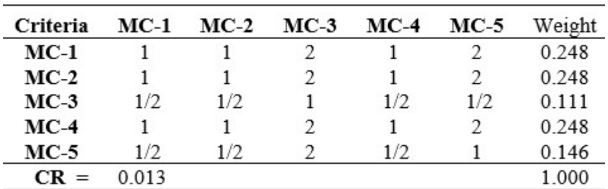
Table 6: Pairwise comparison matrix aggregation for Maritime Operation variable.



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

Source: Authors.

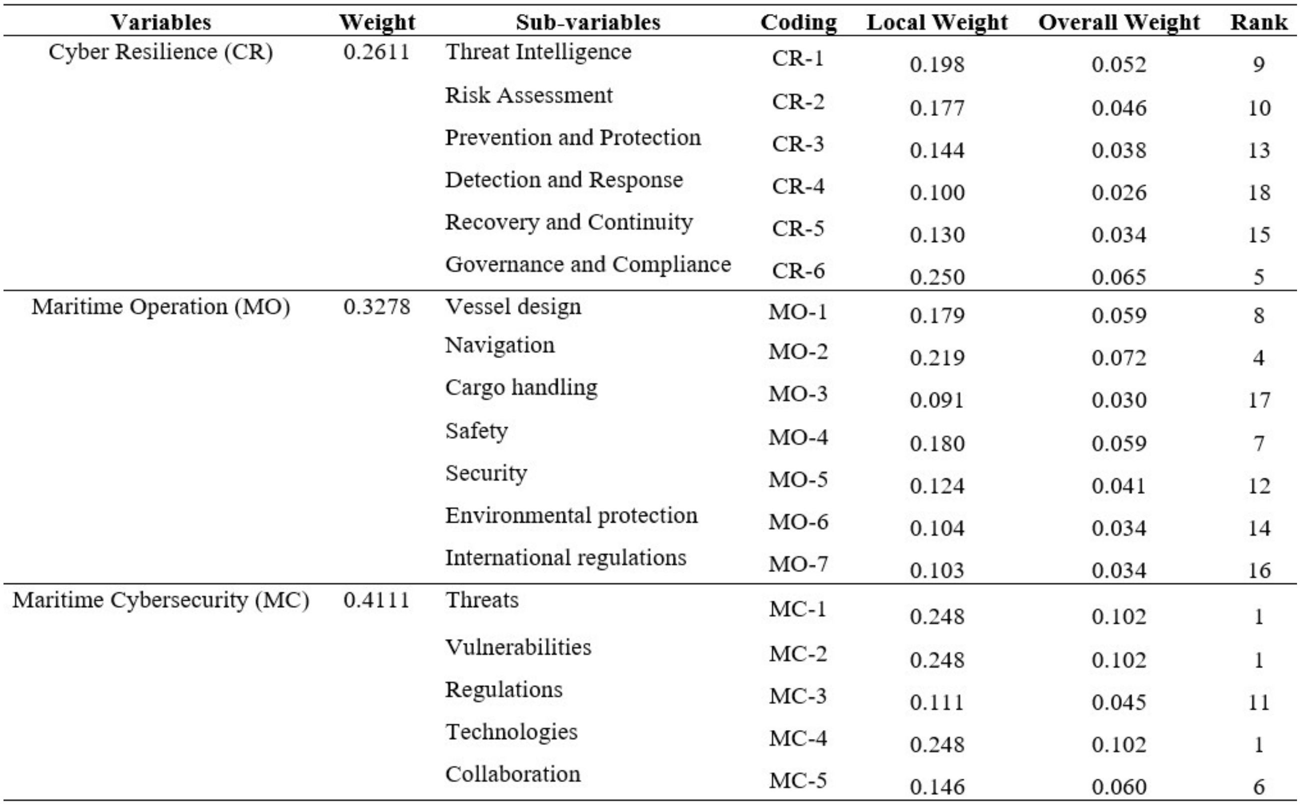
Table 7: Pairwise comparison matrix aggregation for Maritime Cybersecurity variable.



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

Source: Authors.

Table 8: Local Weight and Global Weight for each Variable and Sub-variable of maritime cyber security.



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

Source: Authors.

From Table 4 it can be seen that the criteria variable that is the priority is the Maritime Cybersecurity (MC) variable with a weight value of 0.4111. Second, the variable maritime Operation (MO) with a weight of 0.3278. Third, the variable Cyber Resilience (CR) with a weight of 0.2611. Maritime cybersecurity has attracted increasing, accelerating attention in recent years (Oruc, 2022) and requires a holistic approach due to the increasing complexity, digitization, and automation of systems in the maritime industry (Mraković and Vojinović, 2019) as well as being a problem and requiring attention quickly (Karamperidis, Kapalidis and Watson, 2021). Through collaboration between industry, government and academia, maritime cybersecurity performance can be significantly and efficiently improved (Kanwal et al., 2022). On the other hand, private companies need to dedicate a large part of their budget to addressing maritime cyber security issues (Afenyo and Caesar, 2023). Scientists play a role in developing and implementing maritime cybersecurity methods and policies to ensure the safe operation of ships and enhance the security of the marine environment (McGillivary, 2018). Therefore, the aspect of maritime cyber security is the most influential variable in maritime cyber resilience.

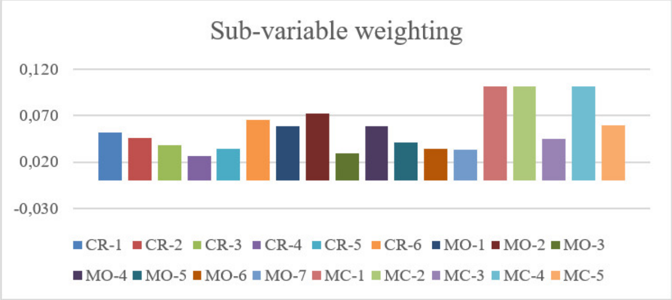
The Cyber Resilience aspect in Table 5, the Governance and Compliance (CR-6) sub-variable is a top priority with the highest weight of 0.250. While the Detection and Response (CR-4) sub-variable with the lowest weight is 0.026. Aspects of Maritime Operations (MO) In Table 6, the Navigation sub-variable (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 7, the Threat (MC-1), Vulnerability (MC-2), and Technologies (MC-4) sub-variables each weight of 0.248 as the highest weight value.

4.3. Consistency test results.

To find out the consistency of the data from the completed questionnaire, a consistency test of the comparison matrix was carried out for each method before calculating the total weight of each variable/criteria. The consistency test in the AHP method is denoted by CR (Consistency Ratio), the data will be consistent if the CR value ≤ 0.1 and if it is more than 0.1 then the data is inconsistent (Sharma et al., 2019; Arora et al., 2020; Maletič et al., 2021). Based on the calculation results, it can be seen that the consistency test using the AHP method found that each variable and sub-variable (Table 4; Table 5; Table 6; Table 7) has a CR value <0.1, so the results of pairwise comparisons are declared consistent.

Local weight and global weight. Local weights and global weights of factors and sub-factors are shown in Table 8. The AHP process makes it possible to incorporate assessments on intangible qualitative criteria in addition to tangible quantitative criteria. This method uses pairwise comparisons of the main criteria and pairwise comparisons of several sub-criteria for each main criterion. After carrying out pairwise comparisons of the main criteria and sub-criteria, the global weight of the sub-criteria is known by multiplying the local weight of the sub-criteria with the weight of the main criteria. After all, weights are calculated following the four steps, local weights and global weights are then calculated. The local weights show the relative importance of the factors within the group, while the global weights show the priority of the factors to Maritime cyber resilience. From this global weight, conclusions can be drawn about the ranking of the importance of the sub-criteria according to the opinion of the decision-makers (Sharma et al., 2019). In practice, obtaining weights can be done, for example by asking for weights directly, in this case it is important to ensure that the weights also reflect the range of criterion values as in research Mustajoki et al., (2020).

Figure 3: Global weight of Sub-variable maritime cyber resilience.



Source: Authors.

Table 8 and Figure 3 describe the local and global weights and the overall ranking of each of the main criteria and sub-criteria. The results of the AHP methodology in research with global weights revealed that the Threat (MC-1), Vulnerability (MC-2), and Technologies (MC-3) sub-criteria were considered the most important, with a global weight of 0.102 each followed by the Navigation (MO) sub-criteria. -2) and Governance and Compliance (CR-6) with a global weight of 0.072 and 0.065 respectively. The Detection and Response (CR-4) sub-criteria ranks last in the pairwise comparisons.

The rapid and continuous progress and development of information technology have increased the complexity of digital systems, which makes systems less secure and thus leads to complexity and changes in the form and function of cyber threats (Aljuhami and Bamasoud, 2021). Organizational resilience is an organization's ability to withstand failure so that it can face potential threats and survive and thrive (Steingartner, Galinec and Kozina, 2021). Internet-connected onboard workstations running 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 from cyber threats (Rios Insua et al., 2021).

Conclusions.

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. Providing an assessment and model simulation of cyber security in the maritime domain is the aim of this article. Based on the research results, this article describes the three criteria and eighteen sub-criteria that affect maritime cyber resilience.

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 a global weight of 0.102 each followed by the Navigation sub-criteria (MO-2). and Governance and Compliance (CR-6) with a global weight of 0.072 and 0.065 respectively. The maritime cyber resilience evaluation value consists of three main criteria. Therefore, to effectively counteract risks to the maritime industry and shipping companies, it is necessary to build a multi-layered cyber security system that meets high standards to protect the supply chain including ships in the process of sea transportation and to keep abreast of risks.

Limitation & Future Work.

This study presents an identify of maritime cyber resilience by analyzing related criteria and assigning weights to priority sub-criteria. The next step in managing maritime cyber resilience is by focusing on threats related to maritime resilience and identifying strategic steps. This provides a basis for the development of new decision-making methods to realize the optimal risk-based selection of security measures or implementation of a sustainability strategy. Second, the main limitation is the survey result of the number of participants. In addition, it is beneficial to hear comments from those who claim to know the maritime and cyber fields. Future work may push this survey to a wider audience with a quantitative approach.

Third, the accuracy of the measurement depends on the selection of maritime cyber resilience criteria and sub-criteria that make up the Resilience Matrice (RM), how reliable and trustworthy the organization's data is, which can be interpreted as organizational bias; implying it may affect the measurement accuracy which is a limitation of this study. For that in the future, it can strengthen data collection techniques by improving algorithms and data structures to reduce bias. Fourth, this study also has not considered cyber-attack scenarios and provides such modeling which is faced with the dynamics of resilience. Therefore, further research is needed to include the attack aspect, multiple attackers with multiple targets, and various attack scenarios not covered in this paper and consider more network-level defense strategies as future research.

Acknowledgements.

This research was supported by by Brawijaya University, and Indonesia Naval Technology College.

References.

Afenyo, M. and Caesar, L. D. (2023) 'Maritime cybersecurity threats : Gaps and directions for future research', Ocean and Coastal Management, 236(November 2022), p. 106493. doi: 10.1016/j.ocecoaman.2023.106493.

Akpan, F. et al. (2022) 'Cybersecurity Challenges in the Maritime Sector', Network, 2(1), pp. 123–138. doi: 10.3390/network2010009.

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. doi: 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. doi: 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. doi: 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. doi: 10.1108/HESWBL-03-2020-0051.

Boyes, H. A. (2014) 'Maritime Cyber Security – Securing the Digital Seaways', Engineering & Technology Reference, (January 2014). doi: 10.1049/etr.2014.0009.

Caprolu, M. et al. (2020) 'Vessels Cybersecurity: Issues, Challenges, and the Road Ahead', IEEE Communications Magazine, 58(6), pp. 90–96. doi: 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(May 2019), pp. 64–75.

Carías, J. F. et al. (2020) 'Systematic approach to cyber resilience operationalization in SMEs', IEEE Access, 8, pp. 174200–174221. doi: 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. doi: 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. doi: 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. doi: 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(January), p. 107934. doi: 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). doi: 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. doi: 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. doi: 10.1007/s-10669-020-09790-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. doi: 10.3390/s22-134895.

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. doi: 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/2-435722737/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). doi: 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. doi: 10.1016/j.cose.2021.1-02196.

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

Hausken, K. (2020) 'Cyber resilience in firms, organizations and societies', Internet of Things (Netherlands), 11, pp. 1–9. doi: 10.1016/j.iot.2020.100204.

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. doi: 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. doi: 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(February), pp. 19–27. doi: 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. doi: 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. doi: 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. doi: 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. doi: 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). doi: 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). doi: 10.3390/jmse9121323.

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. doi: 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). doi: 10.1186/s-11782-020-00083-5.

Kim, K. and Kim, B. (2022) 'Decision-Making Model for Reinforcing Digital Transformation Strategies Based on Artificial Intelligence Technology', Information (Switzerland), 13(5). doi: 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%0Ahttp://-aisel.aisnet.org/confirm2015%0Ahttp://aisel.aisnet.org/confirm-2015/32%0Ahttp://aisel.aisnet.org/cgi/viewcontent.cgi?article=-1015&context=confirm2015%0Ahttps://doc-00-14-docs.googleusercontent.com/docs/secure.

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). doi: 10.3390/fi15010011.

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. doi: 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. doi: 10.3390/s21093195.

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. doi: 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). doi: 10.3390/-safety7010010.

Marzouk, M. and Sabbah, M. (2021) 'AHP-TOPSIS social sustainability approach for selecting supplier in construction supply chain', Cleaner Environmental Systems, 2(March), p. 100034. doi: 10.1016/j.cesys.2021.100034.

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. doi: 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. doi: 10.4031/M-TSJ.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. doi: 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. doi: 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(April 2019), p. 101049. doi: 10.1016/j.ecoser.2019.101049.

Oruc, A. (2022) 'Ethical Considerations in Maritime Cybersecurity Research', TransNav, 16(2), pp. 309–318. doi: 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. doi: 10.1016/j.ocecoaman.2023.106480.

Peter, A. S. (2017) 'Cyber resilience preparedness of Africa's top-12 emerging economies', International Journal of Critical Infrastructure Protection, 17, pp. 49–59. doi: 10.1016/j.ijcip.20-17.03.002.

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. doi: 10.3390/jmse9020112.

Raicu, A. and Raicu, G. (2021) 'Digital Enterprise and Cyber Security Evolution', Macromolecular Symposia, 396(1). doi: 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. doi: 10.1016/j.eij.2022.03.001.

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

Rios Insua, D. et al. (2021) 'An Adversarial Risk Analysis Framework for Cybersecurity', Risk Analysis, 41(1), pp. 16–36. doi: 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. doi: 10.1007/978-94-024-1123-2_14.

Saaty, T. L. (2006) 'There is no mathematical validity for using fuzzy number crunching in the analytic hierarchy process', Journal of Systems Science and Systems Engineering, 15(4), pp. 457–464. doi: 10.1007/S11518-006-5021-7.

Saaty, T. L. (2012) 'The seven pillars of the analytic hierarchy process', International Series in Operations Research and Management Science, 175, pp. 23–40. doi: 10.1007/978-1-4614-3597-6_2.

Seetharaman, A. et al. (2021) 'Impact of Factors Influencing Cyber Threats on Autonomous Vehicles', Applied Artificial Intelligence, 35(2), pp. 105–132. doi: 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. doi: 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. doi: 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. doi: 10.1108/BIJ-08-2018-0253.

Siekelova, A., Podhorska, I. and Imppola, J. J. (2021) 'Analytic Hierarchy Process in Multiple–Criteria Decision–Making: A Model Example', SHS Web of Conferences, 90, p. 01019. doi: 10.1051/shsconf/20219001019.

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. doi: 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. doi: 10.1016/j.system.20-18.03.010.

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

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. doi: 10.1080/23738871.2018.1513053.

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. doi: 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. doi: 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. doi: 10.1007/s10207-021-00545-8.