Contents lists available at GrowingScience

Decision Science Letters

homepage: www.GrowingScience.com/dsl

A hybrid AHP-TOPSIS for risk analysis in maritime cybersecurity based on 3D models

I N. Putra[a], Amarulla Octavian[a], A.K. Susilo[b*] and A. R. Prabowo[c]

[a]Departement of Science and Technology, Indonesia Defense University, Bogor 10430, Indonesia
[b]Departemen Airlangga University, Airlangga-Gubeng, Surabaya 60115, Indonesia
[c]Indonesia Naval Technology College, Moro-Krembangan, Surabaya 60178, Indonesia

CHRONICLE

Article history:
Received: January 12, 2023
Received in revised format:
June 2, 2023
Accepted: June 28, 2023
Available online:
June 28, 2023

Keywords:
Maritime Cybersecurity (MCS)
Risk Analysis
3D Model
Analytical Hierarchy Process (AHP)
Technique for Order by Similarity to Ideal Solution (TOPSIS)

ABSTRACT

Emerging maritime cyber threats put Indonesia's marine technology-based systems at risk This study aims to determine the dimensions and analysis of risk assessment in maritime cyber security based on 3D models in the Indonesian sea area. A statistical descriptive qualitative method approach supported by the Analytical Hierarchy Process (AHP) and Technique for Order by Similarity to Ideal Solution (TOPSIS) methods were used in this study. Risk analysis in maritime cybersecurity has 3 (three) main criteria: Threat, Vulnerability, and consequence. Based on the results of 3D risk analysis, the six dimensions of MCS are identified as having a level of risk at Very Low and Low Risk. The highest risk value is obtained by the dimension of Cyber security-related company procedures (D2) (0.368) and the lowest risk value is Ship's systems readiness (D3) (0.048).

1. Introduction

Indonesia has historically had a very dominant influence in the Southeast Asian region and even the entire Asian region. The area of Indonesia, which is two-thirds of its sea area, has the potential to unite and become a source of conflict between regions or countries, including in the national maritime aspect (Subagyo, 2018). As the largest nation made up of islands, Indonesia is situated in a geographically advantageous region that separates the Pacific and Indian Oceans and is sandwiched between the continents of Asia and Australia (Marnani et al., 2021). Because it is the world's biggest archipelago, with 17,508 islands (large and small), between 2000 and 4000 of which are inhabited, and because around two-thirds of the country's land area is water, Indonesia is regarded as a Global Maritime Fulcrum (Mursitama & Ying, 2021). Maritime cyber risk refers to the extent to which a potential state of affairs threatens a technology asset. This can result in operational, safety or security failures in shipping as a result of damaged, lost or disrupted information or systems (Desiana & Prima, 2022). Haugli et al. (2022) explained the need to provide risk assessment analysis on maritime cybersecurity. Afenyo & Caesar (2023), recommends the need for future research for risk analysis using a qualitative method approach to the in-depth understanding of the main factors driving risks/attacks on maritime cybersecurity. Bolbot et al. (2020), recommends the need for future research initiatives on improving the accuracy of ratings and aggregating different risk scores on maritime cybersecurity. Noor (2022), explains the need for an analysis of risk assessment in the maritime cyber industry as a standard for cyber security. Larsen and Lund (2021), recommends the need to investigate dimensions in viewing the maritime cybersecurity domain. Yoo and Park (2021), provides several recommendations regarding cybersecurity in the maritime sector in a pairwise comparison with MCDM.

* Corresponding author.
E-mail address: april.kukuh.susilo-2020@feb.unair.ac.id (A.K. Susilo)

doi: 10.5267/dsl.2023.6.005

This study aims to investigate the dimensions and analysis of risk assessment in maritime cybersecurity by using a qualitative method approach based on 3D models. It is important to pay more attention to the behavior that occurs in maritime cyber security and to understand how we can enable maritime cyber security systems. Understanding insights related to risks in maritime security, and risk mitigation, can enrich the literature and appropriate risk consequences. This research provides insight into mitigating maritime security threats and increases security awareness in implementing management policies for the level of risk of cybersecurity threats. This research is also a valuable tool for conducting risk assessments in maritime cybersecurity and supporting cost-benefit analysis. This study uses a statistical descriptive qualitative method approach supported by the AHP and TOPSIS methods. First, this research identifies the risk elements in maritime cybersecurity. Second, provide a risk analysis of the maritime cybersecurity elements which are described with a risk map based on a 3D model. This research provides several contributions. First, maritime domain cyber security risk assessment provides an additional contribution to the field of risk management. Second, the use of research methods provides direction in risk assessment and enriches the maritime cybersecurity analysis literature. Third, the research evaluates the variables and obtains a value for each potential threat and risk from the expert's opinion and presents their judgment so that their initial evaluation can be considered balanced, and indicates directions for further analysis.

This research consists of several parts. Section 2 describes a literature review consisting of Maritime Security, Cybersecurity, Maritime Cybersecurity (MCS), and Risk Assessment. Section 3 describes the methodology which consists of research design, conceptual framework, AHP and TOPSIS method, and 3D risk analysis model. Section 4 describes the results & discussion which consists of identification of criteria and alternatives, Maritime Cybersecurity Risk Analysis. Section 5 is the conclusion of the research including research implications, limitations and future research.

2. Literatur Review

2.1. Maritime Security

Maritime security is a trendy topic. Conditions achieve their meaning through players associating the idea with others, trying to fill it with multiple topics, and taking action to honor it. Even if parties agree that maritime security is important in general, parties, time and space will always influence what that means in practice (Bueger, 2015). Therefore, searching for a definition of maritime security that is considered to be widely accepted has yielded no results. Maritime security can be analyzed similarly by recognizing the relationship with other terms. Maritime security governs the web of relations, replacing or incorporating old, well-established concepts, as well as linking with newly developed ones. At least four of these require consideration: sea power, sea security, blue economy, and human resilience. Each of these concepts directs us to a different dimension of maritime security. The concepts of sea power and sea safety are old understandings of danger at sea, the last two emerged at roughly the same time as maritime security (Bueger & Edmunds, 2020). Maritime security is defined as the protection of national interests, at home and abroad, through the active management of risks and opportunities within and from the maritime domain, to strengthen and expand a nation's prosperity, security, and resilience and to help shape a stable world (Chapsos & Malcolm, 2017). The behavior and interactions of various actors have an impact on maritime security. The notion of maritime security falls between two concepts: organizations that use unconventional frameworks, and groups that use typical security frameworks (Susilo et al., 2019). There are several threats to maritime security, such as; 1) threats of violence (piracy, sabotage, and vital objects of terror); 2) navigation threats; 3) resource threats, such as damage and pollution of the sea and its ecosystem; 4) threat to sovereignty.

2.2. Cybersecurity

Cybersecurity gets a lot of attention because we are constantly surprised by the ubiquitous nature, persistence, diversity and consequences of attacks. Modern information systems exhibit a distinctive dynamic design, and the wide availability of associated technologies creates fertile ground, not only for unpredictable behavior (bugs), but also for innovative malicious actors to discover and exploit new failure modes and attack vectors (Roege et al., 2017). Cybersecurity is not only about preventing hackers from accessing systems and information but also about protecting digital assets and data, ensuring business continuity, and securing the maritime industry from external and internal threats. Cyber incidents can last hours, days or weeks (Desiana & Prima, 2022). Cybersecurity is no longer just the domain of IT departments (Malatji et al., 2022). Cybersecurity is an important facilitator of digitization, but if managed improperly it can undermine all its benefits (Ghelani, 2022). Cybersecurity is generally defined as the protection of cyberspace as well as the individuals and organizations that function within cyberspace and their assets in that space (Changki Park et al., 2019). Cybersecurity can also be defined as a collection of tools, policies, security safeguards, guidelines, risk management approaches, training, best practices, assurance, and technology used to protect the cyber environment and organizational assets (Lykou et al., 2019; Tissir et al., 2021).

2.3. Maritime Cybersecurity (MCS)

Cybersecurity is a relatively new concept for shipping, it is not yet understood, and most maritime operators and managers have no training regarding cyber risks (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 et al., 2021). Maritime Cybersecurity is a combination of the two terms 'maritime security' and 'cyber security'. first term; maritime security, it has been argued that it 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 also depends 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 and are categorized as the basis that affects maritime cybersecurity performance (Kanwal et al., 2022) likely Regulatory framework; Cyber security-related company procedures; Ship's systems readiness; Cyber training and awareness; Compliance monitoring; Human factors.

2.4. Risk Analysis

Risk assessment is the entire process of risk identification, risk analysis and risk evaluation. Risk can be assessed at the organizational level or departmental level for a particular project, individual activity or risk. Different tools and techniques may be appropriate in different contexts. Risk assessment provides an understanding of risks, their causes, consequences, and probabilities. Risk analysis is about developing an understanding of risk (Valis & Koucky, 2009). Risk analysis is an important methodology for cybersecurity because it allows organizations to deal with cyber threats that have the potential to affect them, prioritize the defense of their assets, and decide what security controls to implement. Many risk analysis methods are present in cybersecurity models, compliance frameworks and international standards (Insua et al., 2021).

The risk analysis can be written with the risk formula adopted by Chang et al. (2021); Octavian et al. (2020):

$$\text{Risk (R)} = \text{Threat (T)} \times \text{Vulnerability (V)} \times \text{Consequence (C)} \tag{1}$$

Table 1
Value of Risk Analysis Level of Each Criteria

Likert	Risk Analysis Level		
Score	Threat	Vulnerability	Consequence
5	Very High	Very High	Catastrophic
4	High	High	Critical
3	Moderate	Medium	Moderate
2	Low	Low	Marginal
1	Very Low	Very Low	Negligible

Adopted from Kure et al. (2018) and Octavian et al. (2020).

Table 2
Rating of the Level Value for Each Risk Analysis Criteria

Likert	Description of Risk Analysis		
Score	Threat	Vulnerability	Consequence
5	State-sponsored assaults are carried out for economic domination, information control, or national instability.	One or more major weaknesses have been identified that make the asset extremely susceptible to an attack. The organization has no capability of resisting the occurrence of a threat	The threat causes a total system loss. An extremely serious consequence that affects sailing operations occurs
4	Cyber sabotage, also known as industrial espionage, is a danger posed by industry rivals and market competitors, who frequently attack the target company's intellectual property.	One or more major weaknesses have been identified that make the asset highly susceptible to an attack. The organization has a low capability of resisting the occurrence of a threat	The threat causes major system damage. The system operations need to be stopped. High degree of operational interruption occurs
3	Cyberattacks may also be launched for illicit purposes by individuals or criminal groups.	A weakness has been identified that makes the asset moderately susceptible to an attack. The organization has the reasonable capability of resisting the occurrence of a threat	The threat causes moderate system damage. The system operations are interrupted. It requires a longer period (e.g., more than 12 h) to fix the system. The threat causes a major system damage
2	Cyber thieves, also called Terrorist groups, are frequently created by particular religious, political, and social ideas and target opposing groups, nations, and countries through their acts.	A minor weakness has been identified that slightly increases the susceptibility of the asset to an attack. The organization has a good capability of resisting the occurrence of a threat	The threat causes marginal system damage. The system operations are slightly interrupted. It requires a short period (e.g., less than 6 h) to fix the system
1	Representing an ideological motivation, such individuals/groups steal sensitive information to exploit their target.	No weaknesses exist. The organization has an excellent capability of resisting the occurrence of a threat.	The consequence of the threat is limited. It only requires a minor maintenance

Adapted from Kure et al. (2018); Octavian et al. (2020); Park et al. (2023)

Table 3
Risk Level of Maritime Cybersecurity

Level	Score	Risk Level	Description
5	0.800-1	Extreme	The risk level is extremely critical and requires the implementation of control measures to mitigate risk almost immediately. The risk level is extremely critical when the threat, vulnerability, and consequence of the risk event is extreme. Could result in serious damage that could obstruct the operations of the organization.
4	0.600-0.799	High	The risk level is highly critical and requires the implementation of the control measures for mitigating risk that has to be immediately within a short time frame. The risk impact is highly critical when the threat, vulnerability, and consequence of the risk event are extreme and/or high. Expected to have a serious impact on the organization's reputation.
3	0.400-0.599	Medium	The risk level implies that the risk has an adversarial effect on the organization and effective actions need to be applied to the contingency plan of the organization and within a specific period. It is likely to result in a short-term disruption of the organization's services.
2	0.200-0.399	Low	The risk level from the risk event requires the organization to take effective actions and may require the need for a new contingency plan as well as corrective measures.
1	0.1-0.199	Very Low	This risk level indicates that a corrective measure needs to be implemented and a contingency plan needs to be developed.

Modified from Ashraf et al. (2022); Bodeau et al. (2010); Malatji et al. (2022)

3. Methodology

This research was conducted in the Indonesian sea area which is part of Maritime Cybersecurity. The purpose of this study is to provide an assessment of the risks to Maritime Cybersecurity in Indonesian seas from cyber-attacks which are a current phenomenon. This research is a qualitative descriptive statistical research by applying a decision-making method with two stages of multiple criteria: a) analytical hierarchical process (AHP) and b) TOPSIS. Dimensions of risk analysis on MCS and priorities are calculated using the AHP method, which is then analyzed with TOPSIS to provide risk classification and map it in a 3D risk matrix as Octavian et al. (2020).

Questions related to risk analysis were framed on a five-point Likert scale ranging from 1 to 5 in Table 1. Eight experts were selected as Tseng et al. (2022), regarding the cyber-maritime field through purposive sampling contacted via email and google form (Akter et al., 2022) for data collection. Most of the experts in this study are high-ranking officials in the maritime field. Consulted with two experts (two high-ranking officials who have worked for more than 5 years) and two doctorates for maritime cybersecurity competence. Their opinions and suggestions helped the authors build a threat hierarchy and refine the risk analysis model.

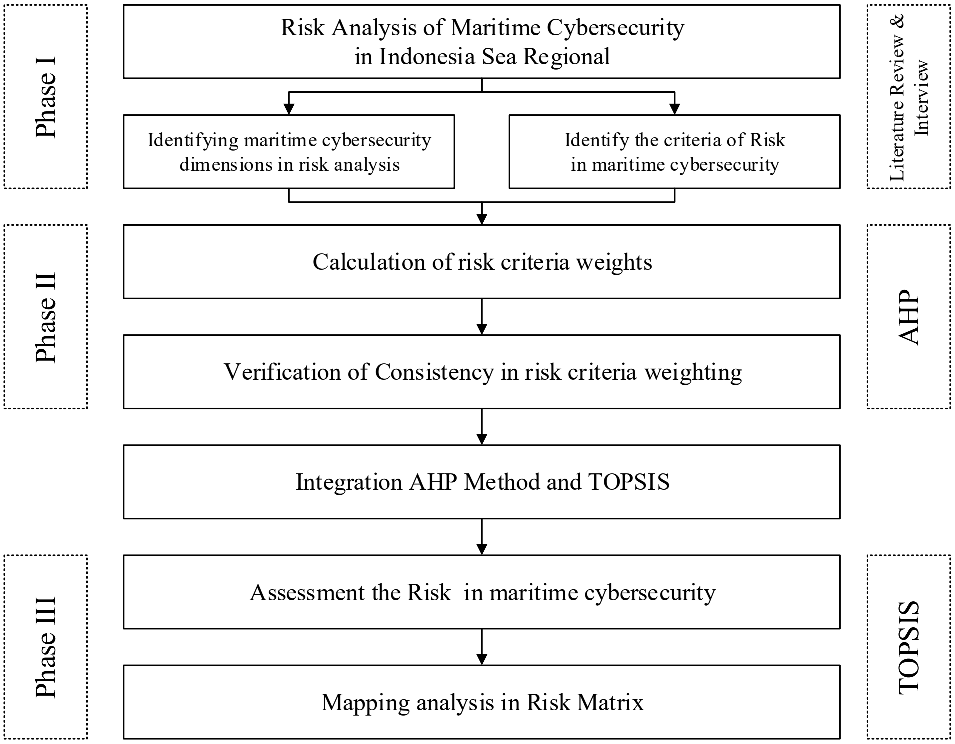
Phase I
Risk Analysis of Maritime Cybersecurity in Indonesia Sea Regional
Identifying maritime cybersecurity dimensions in risk analysis
Identify the criteria of Risk in maritime cybersecurity
Literature Review & Interview
Phase II
Calculation of risk criteria weights
Verification of Consistency in risk criteria weighting
AHP
Integration AHP Method and TOPSIS
Phase III
Assessment the Risk in maritime cybersecurity
Mapping analysis in Risk Matrix
TOPSIS

Fig. 1. Conceptual framework of Risk Analysis in Maritime Cybersecurity
Adopted from Biancini (2016) and Singh & Sarkar (2019)

The proposed conceptual framework of this research is presented in Fig. ***1***. The research objectives consisted of three parts, including:

- Identifying criteria and alternative of risk to Maritime Cybersecurity;
- Analyzing, measuring, and mapping the level of risk to Maritime Cybersecurity using the AHP-TOPSIS approach;

This research also develops a model capable of providing an assessment and measurement of the level of risk in Maritime Cybersecurity. It should be noted that the TOPSIS and AHP techniques are used because of several advantages, as were Marzouk & Sabbah (2021) and Saini & Singh (2022). The model mechanism illustrated in the flowchart shown in Fig. 1 was divided into three modification phases by Menon & Ravi (2022) and Boutkhoum et al. (2017).

Phase 1 – This article considers risk assessment in maritime cybersecurity, and defines the criteria, and dimensions of maritime cybersecurity through a review of the literature and discussions with experts to produce an overview of all the criteria that need to be considered when making decisions. This stage ends when a consensus on the criteria and types of maritime cybersecurity dimensions has been reached.

Phase 2 – Through a literature review and expert opinion, the criteria and dimensions of maritime cybersecurity are identified. Questionnaires were given to get responses in identifying criteria and produce a hierarchical structure and followed by calculating the relative importance/weight of these criteria.

Phase 3 – Analysis of risks to maritime cybersecurity is evaluated based on the parameters against the criteria. TOPSIS was adopted to rank and measure the value of the level of risk in the decision-making process as well as map the risk matrix.

3.1. Analytical Hirarchy Process (AHP)

AHP was developed by Saaty (2008) as a model for solving decision problems. AHP ensures that quantitative and qualitative variables can be evaluated together by considering the priorities of the decision-makers. The stages in the AHP process can be summarized as follows:

- The purpose of the problem is defined.
- The decision hierarchy framework is drawn according to the alternatives.
- Pairwise comparisons of criteria are made, and pairwise comparison matrices are developed.
- Benchmark weights are obtained from the pairwise comparison matrix.
- Consistency of specified benchmark weights is taken into account

The steps of the method can be given as follows:

- Arranging decision situations into goals, decision criteria, and alternatives.
- Creating questionnaires and collecting data. Comparisons are made for each criterion and converted into quantitative figures using linguistic terms.
- Generating pairwise comparisons for various criteria.
- Determining the weight of each criterion.
- Conducting consistency analysis. The consistency ratio is calculated based on the following steps:
    - The consistency index (CI) is determined through

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

where λ_{max} is the maximum eigenvalue of the judgment matrix.

- Then, the final consistency ratio (CR) is obtained from

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

Table 4
Random consistency index (RI)

n	1	2	3	4	5	6	7	8

Random Index (RI)	0	0	0.58	0.9	1.12	1.24	1.32	1.41

Source: Octavian et al. (2020); Solangi et al. (2019)

If the CR ratio ≤ 0.1 (i.e. 10%), the matrix was said to be consistent decision was accepted. Conversely, CR more than implied too many contradictions in the matrix. The anticipation for the final situation was to review the matrix, and then revise the weights loaded by the vector.

3.2. TOPSIS

TOPSIS is a multicriteria decision analysis method, which was originally developed by Hwang and Yoon (1981) with further development by Yoon in 1981. This method is based on the concept that the chosen alternative must have the shortest distance from the positive ideal solution (PIS) and the farthest distance from the negative ideal solution (NIS). The TOPSIS method is often used because it is easy to calculate, understand, and allows alternative performance evaluations with simple mathematical models. The main steps of the TOPSIS method are given as follows:

The Likert scale is first modified into an interval scale using Microsoft Excel to analyze the questionnaire results. Then the weights for each criterion and alternative were calculated using geometric averages (Octavian et al., 2020). These geometric mean values are considered the result of group assessments of the values given by 18 experts (Çalık et al., 2019).

a. Creating a matrix of terrorism risk analysis decision-making.
b. Normalizing the decision matrix.

$$X = \begin{bmatrix} X_{11} & X_{12} & \dots & X_{1n} \\ X_{21} & X_{22} & \dots & X_{2n} \\ \dots & \dots & \dots & \dots \\ X_{m1} & X_{m2} & \dots & X_{mn} \end{bmatrix} \tag{4}$$

$$r_{ij} = \frac{X_{ij}}{\sqrt{\sum_{k=1}^{m} X_{kj}^2}} \tag{5}$$

c. Multiplying the risk matrix with the weight of each AHP criterion.

$$y_{ij} = w_j x r_{ij} \tag{6}$$

where *i=1,..., m* and *j=1,..., n*.

$$Y = \begin{bmatrix} w_1 & w_2 & \dots & w_m \end{bmatrix} \begin{bmatrix} r_{11} & r_{12} & \dots & r_{1n} \\ r_{21} & r_{22} & \dots & r_{2n} \\ \dots & \dots & \dots & \dots \\ r_{m1} & r_{m2} & \dots & r_{mn} \end{bmatrix} = \begin{bmatrix} w_1 x\, r_{11} & w_2 x\, r_{12} & \dots & w_n x\, r_{1n} \\ w_1 x\, r_{21} & w_2 x\, r_{22} & \dots & w_n x\, r_{2n} \\ \dots & \dots & \dots & \dots \\ w_1 x\, r_{m1} & w_2 x\, r_{m2} & \dots & w_n x\, r_{mn} \end{bmatrix} \tag{7}$$

d. Determining a positive ideal solution matrix and a negative ideal solution matrix.

$$A^- = (y_1^-, y_2^-, \dots\dots, y_n^-)$$
$$A^+ = (y_1^+, y_2^+, \dots\dots, y_n^+) \tag{8}$$

Based on normalized weight, the positive ideal solution A+ and the ideal solution A- may be established (yij). Multiplying the weights of the internal service quality dimension criteria with the normalized matrix will yield the normalized weight decision matrix. Based on the normalized weight, the positive ideal solution A+ and the negative ideal solution A- may be derived (yij). Following the calculation of the value of a positive ideal solution (A+), the value of a negative ideal solution (A-) is also determined.

e. Determining the distance of each alternative (Erdogan & Kaya, 2019).

$$D_i^- = \sqrt{\sum_{j=i}^{n}\left(y_{ij} - y_j^-\right)^2} \text{ and } D_i^+ = \sqrt{\sum_{j=i}^{n}\left(y_{ij} - y_j^+\right)^2} \tag{9}$$

f. Calculating the value of risk preferences of each alternative following the results of decision-makers (Sharma & Sehrawat, 2020).

$$V_i = \frac{D_i^-}{D_i^- + D_i^+} \tag{10}$$

Based on how close each alternative is to the ideal solution, the preference value for each option (Vi) can be determined.

Table 5
Scale of pairwise comparison for AHP and Likert scale for TOPSIS

Scale	Description	Likert	Risk Level
9	The evidence favoring one activity over another is the highest possible order of affirmation (absolutely more important)	5	Extreme
7-8	An element is favored very strongly over another, and its dominance is demonstrated in the practice (demonstrated importance)	4	High
5-6	Experience and judgement strongly favor one element over another (essential, strong more important)	3	Medium
3-4	Experience and judgement slightly favor one element over another (moderately more important)	2	Low
1-2	Two elements contribute equally to the objective (equal importance)	1	Very Low

Source: modified from Octavian et al. (2020; Susilo et al. (2019)

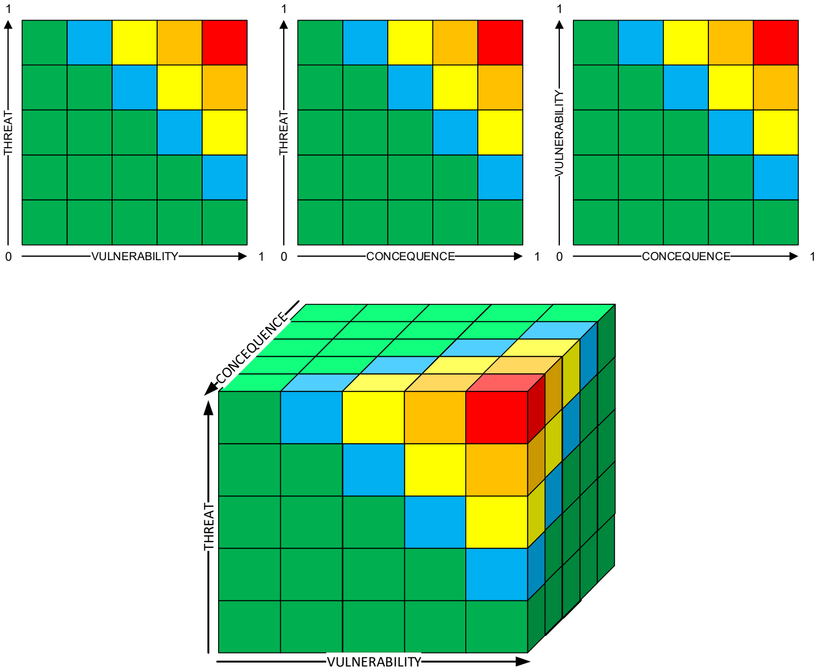

Fig. 2. 3D Risk model of risk analysis in Maritime Cybersecurity.

Modified from Amirshenava & Osanloo (2018); Crotty & Daniel (2022); Octavian et al. (2020); Yoo & Park (2021)

4. Result & Discussion

In this section, the proposed framework is used to identify maritime cybersecurity risks and map them in a risk matrix based on risk level values. The first step is to identify from the literature review the risk factors and dimensions of maritime cybersecurity in the event of a cyber attack. The second step is to measure, assess and map the Maritime Cybersecurity risk level.

4.1. Identification of criteria and Alternatives

Identification of criteria in maritime cybersecurity risk analysis was obtained from several previous studies, namely research from Jiang et al. (2023), Yoo & Park (2021), Gunes et al. (2021), and Ganin et al. (2017) as the main reference. The next step is to arrange a hierarchy by compiling objectives, criteria and alternatives. Preparation of criteria and sub-criteria for maritime cybersecurity risk analysis. As for alternatives, there are six dimensions of maritime cybersecurity literature from Alcaide & Llave, (2020); Kanwal et al. (2022); and Progoulakis et al. (2021) such as Regulatory framework (D1); Cybersecurity-related company procedures (D2); Ship's systems readiness (D3); Cyber training and awareness (D4); Compliance monitoring (D5); Human factors (D6).

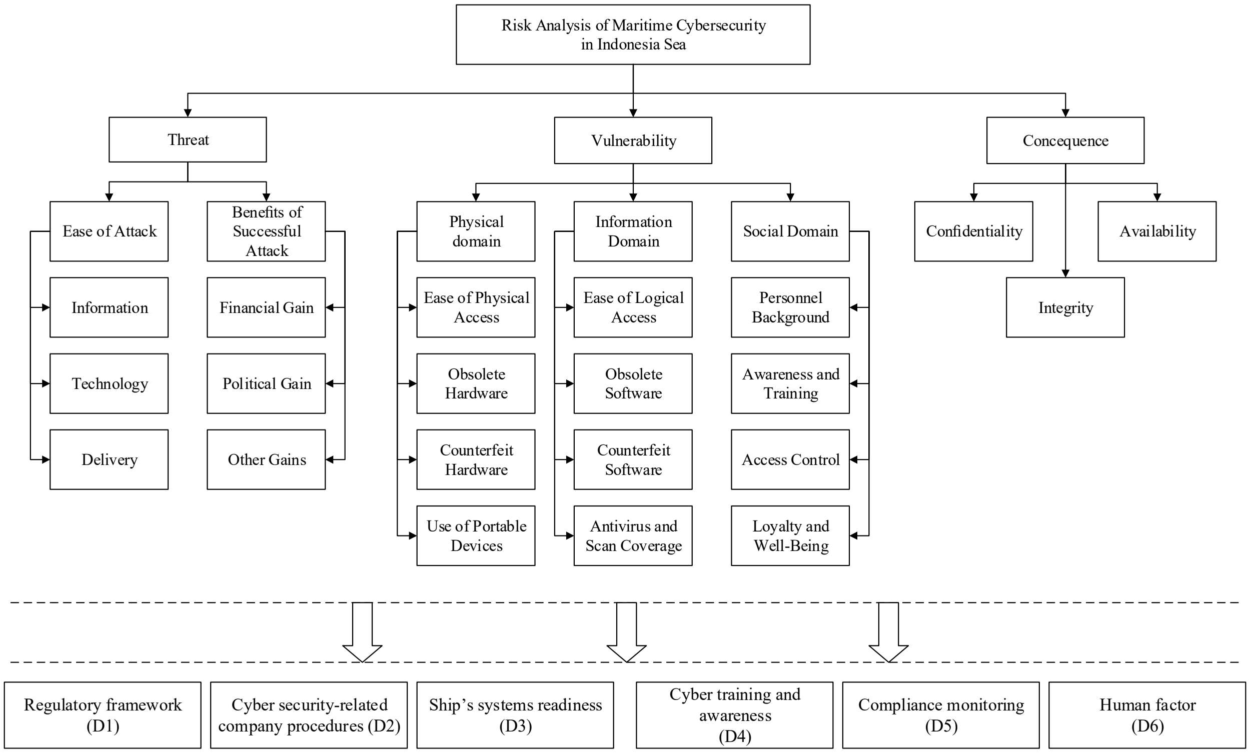

Fig. 3. A hierarchical model of risk analysis in maritime cybersecurity.

Identification of influencing factors or criteria is carried out to determine risk analysis in maritime cybersecurity. Therefore, building a hierarchical structure serves to establish causal relationships between risk factors. Risk analysis in maritime cybersecurity has 3 (three) main criteria: Threat, Vulnerability, and consequence. Threat Criteria has 6 (six) sub-criteria; criteria, vulnerability consists of 12 (twelve) sub-criteria, and consequence consists of 3 (three) sub-criteria. The dimensional aspects of maritime cybersecurity consist of 6 (six) dimensions. All hierarchical factors are shown in Fig. 3.

Table 6
Overall priority weight and ranking of criteria and sub-criteria.

Risk Criteria	Evaluation Sub Criteria	Weight (Prioritized)	Overall Weight (Prioritized)	Rank
Threat		0.4000	1st (Criteria)	
	Information	0.2166	0.0867	3
	Technology	0.2469	0.0988	1
	Delivery	0.0995	0.0398	12
	Financial Gain	0.1958	0.0783	4
	Political Gain	0.1152	0.0461	9
	Other Gains	0.1259	0.0503	8
Vulnerability		0.4000	2nd (Criteria)	
	Ease of Physical Access	0.3199	0.0399	10
- Physical domain	Obsolete Hardware	0.1287	0.0161	19
0.3119	Counterfeit Hardware	0.2314	0.0289	15
0.1248	Use of Portable Devices	0.3199	0.0399	10
- Information Domain	Ease of Logical Access	0.3873	0.0760	6
0.4905	Obsolete Software	0.1397	0.0274	16
0.1962	Counterfeit Software	0.1981	0.0389	13
	Antivirus and Scan Coverage	0.2748	0.0539	7
- Social Domain	Personnel Background	0.2002	0.0158	20
0.1976	Awareness and Training	0.1418	0.0112	21
0.0790	Access Control	0.3290	0.0260	17
	Loyalty and Well-Being	0.3290	0.0260	17
Consequences		0.2000	3rd (Criteria)	
	Confidentiality	0.3873	0.0775	5
	Integrity	0.1698	0.0340	14
	Availability	0.4429	0.0886	2

After compiling the section on the importance of key factors influencing a valid questionnaire, C.I. value 0.02, and value C.R. is 0.023 for the 3 main criteria and 21 assessment sub-criteria, indicating that a valid questionnaire meets the consistency standard. The relative importance of the key factors influencing risk analysis in maritime cybersecurity (MCS) is shown in Table 6. Results of the AHP methodology in this study reveal that threat and vulnerability criteria are important aspects (40%), while consequence aspects of 20%. Furthermore, of the 21 assessment sub-criteria, there are five of the most important sub-criteria, namely Technology (9.8%), Availability (8.8%), Information (8.6%), financial gain (7.8%), confidentiality (7.7%). The most influential sub-criteria in the risk analysis comes from the threat and consequence criteria. These aspects are correctly identified because they are a challenge for policymakers in Indonesia's marine areas in maintaining maritime cybersecurity.

4.2. Risk Analysis on Maritime Cybersecurity

After establishing the weighting of the risk assessment criteria, a questionnaire selection scheme was compiled from a risk analysis of the six dimensions of maritime cybersecurity to provide an assessment of the threat, vulnerability, and consequence aspects with the positive ideal solution and the farthest from the negative ideal solution, the most appropriate in order of priority using an index scale of 5 steps all variables reach the maximum value.

Table 7
Risk analysis value of threat aspect.

Alternative	D+	D-	Result	Rank	Level
D1	0.027	0.023	0.455	5	Moderate
D2	0.023	0.031	0.567	3	Moderate
D3	0.027	0.026	0.492	4	Moderate
D4	0.036	0.021	0.368	6	Low
D5	0.020	0.030	0.605	2	High
D6	0.019	0.037	0.661	1	High
		Average Level	0.525		Moderate

Based on Table 7, it shows that in the threat aspect among the six dimensions, there are two dimensions at the High level, namely Compliance monitoring (D5), Human factor (D6) with a closeness coefficient of 0.605 and 0.661 respectively. Furthermore, there are three dimensions at the moderate level, namely Regulatory framework (D1), Cyber security-related company procedures (D2), Ship's systems readiness (D3) with each proximity coefficient of 0.455, 0.567, 0.492. There is one dimension in the Low category, namely Cyber training and awareness (D4) with a coefficient of 0.368. Thus, the highest threat aspect is in Compliance monitoring (D5), Human factor (D6). On average, the threat aspect is at a moderate level with a value of 0.525.

Table 8
Risk analysis value of vulnerability aspect.

Alternative	D+	D-	Result	Rank	Level
D1	0.022	0.020	0.486	3	Medium
D2	0.010	0.030	0.742	2	High
D3	0.027	0.019	0.415	6	Medium
D4	0.023	0.017	0.419	5	Medium
D5	0.022	0.019	0.461	4	Medium
D6	0.007	0.031	0.809	1	Very High
		Average Level	0.555		Medium

Table 8 shows that in the aspect of vulnerability among the six dimensions, there is one dimension at the Very High level, namely the Human factor (D6) with a proximity coefficient of 0.809. The Cyber security-related company procedures (D2) dimension is at the High level of 0.742. Furthermore, there are 4 dimensions at the medium level, namely Regulatory framework (D1), Ship's systems readiness (D3), Cyber training and awareness (D4), Compliance monitoring (D5) with each proximity coefficient of 0.486, 0.415, 0.419, 0.461. Thus, the highest vulnerability aspect is in the Human factor (D6). On average, the vulnerability aspect is at a medium level with a value of 0.555.

Table 9
Risk analysis value of consequence aspect.

Alternative	D+	D-	Result	Rank	Level
D1	0.030	0.027	0.472	4	Moderate
D2	0.006	0.043	0.875	1	Catastrophic
D3	0.038	0.012	0.233	6	Marginal
D4	0.026	0.028	0.523	3	Moderate
D5	0.010	0.039	0.799	2	Critical
D6	0.032	0.028	0.467	5	Moderate
		Average Level	0.562		Moderate

Table 9 shows that in the consequence aspect among the six dimensions, there is one dimension at the Catastrophic level, namely Cyber security-related company procedures (D2) with a coefficient value of 0.875. one dimension is Critical level, namely Compliance monitoring (D5) with a coefficient value of 0.799. One dimension at the Marginal level, namely Ship's systems readiness (D3) of 0.233. then three dimensions are at a moderate level, namely Regulatory framework (D1), Cyber training and awareness (D4), and Human factors (D6) with each proximity coefficient of 0.472, 0.523, 0.467. On average, the consequence aspect is at a moderate level with a value of 0.562.

Table 10
Risk Evaluation value of alternative maritime cybersecurity

Dimension	T	V	C	Risk Score	Risk Level
D1	0.455	0.486	0.472	0.104	Very Low
D2	0.567	0.742	0.875	0.368	Low
D3	0.492	0.415	0.233	0.048	Very Low
D4	0.368	0.419	0.523	0.081	Very Low
D5	0.605	0.461	0.799	0.223	Low
D6	0.661	0.809	0.467	0.250	Low

The final step of the criterion risk analysis is determining a reference value to determine the final level of risk. The level of risk is determined by three variables, namely threat (T), vulnerability (V), and consequence (C). Based on this, a 3D model should be used to describe the level of risk. The associated values are determined by a team of experts.

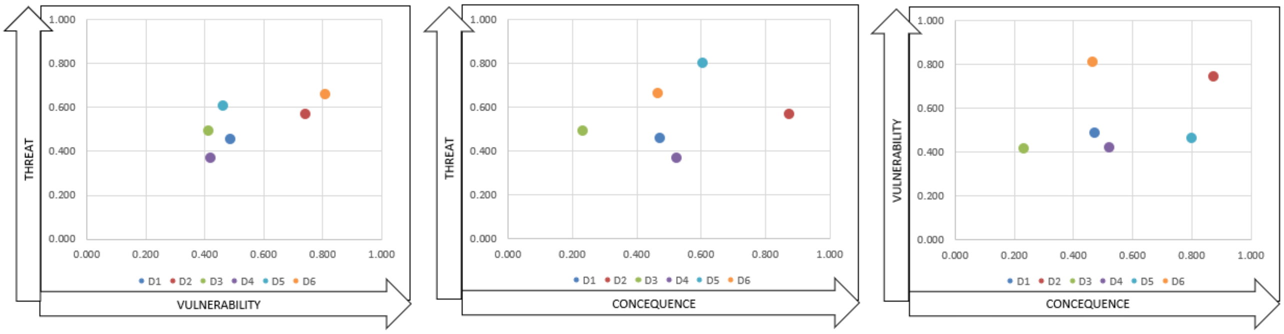

Fig. 4. Results of risk analysis on the 3D Matrix for maritime Cybersecurity.

In Table 10 and Fig. 4, based on the risk calculation results, of the six dimensions of maritime cybersecurity in Indonesia, there are dimensions at Very Low and Low Risk levels. Three MCS dimensions with Low levels are Cyber security-related company procedures (D2), Compliance monitoring (D5), Human factor (D6) with respective risk values of 0.368, 0.223, 0.250. Three other MCS dimensions with very low levels are Regulatory framework (D1), Ship's systems readiness (D3), Cyber training and awareness (D4) with respective risks of 0.104, 0.048, 0.081. The highest risk value is obtained by the Cyber security-related company procedures (D2) dimension and the lowest risk value is Ship's systems readiness (D3). Overall, the risk of attacks on MCS in the Indonesian Sea area is still in the Low category.

Risk management on MCS in Indonesia's sea area mine closure plays an important role in safeguarding activities from and through the sea in line with the vast area of Indonesia which is mostly sea by the dimensions of MCS. In this regard, a risk management approach to maritime Cybersecurity is developed based on a 3D risk model as well as a robust hybrid decision support system, which is developed and implemented for each maritime activity with some modifications to the risk factors and alternative dimensions of MCS applied, based on the specific conditions related to the national marine area conditions. Developing a 3D risk assessment model based on the three factors of threat, vulnerability, and consequences as one of the most important features is considered an advantage of this approach, compared to other similar studies. The results of the AHP and TOPSIS methods in the case study show that the methods are compatible. In other words, the selection of these methods is correct and the most suitable choice.

5. Conclusion

This research uses a 3D risk analysis management developed to investigate the dimensions and risk assessment analysis of maritime cybersecurity in Indonesia's marine areas. The risk assessment approach based on AHP and TOPSIS-based 3D risk matrix becomes a practical and efficient tool to evaluate and rank the risks of MCS dimensions. This framework makes it possible to balance and compare risks associated with maritime cybersecurity elements, as well as to create a database, supplementing it with factual figures to achieve several subcriteria (21 subcriteria in total) and comparison relationships. The ability to adopt new models in the MCS is considered another advantage of the risk analysis approach.

The results of applying this framework to the Indonesian marine domain showed effectiveness compared to 2D risk models. In terms of risk factors, the results of this study show that there are five most important sub-criteria, namely Technology (9.8%), Availability (8.8%), Information (8.6%), financial gain (7.8%), confidentiality (7.7%). The most influential sub-criteria in risk analysis comes from the threat and consequence criteria. Based on the results of the 3D risk analysis, six

MCS dimensions were identified as having risk levels at Very Low and Low Risk levels. The highest risk value is obtained by the Cyber security-related company procedures (D2) dimension (0.368) and the lowest risk value is Ship's systems readiness (D3) (0.048). Overall, the risk of attacks on MCS in the Indonesian Sea area is still in the Low category.

This research has real implications for qualitative analysis of cyber risk management aspects in the maritime domain in Indonesia's maritime region, with technological sophistication increasing every year and increasing risks and threats to the maritime cybersecurity dimension. This research will assist stakeholders in evaluating and developing a 3D model-based maritime cybersecurity risk value framework as a first step in determining policy strategies by adopting the solutions provided in the research. This framework not only helps state actors to identify their capabilities from an objective perspective but also to compare them with their competitors to gain insights to improve competitive advantage.

There are several limitations in the study. First, a cost-benefit analysis should be conducted after selecting a risk treatment option to improve the efficiency of the proposed approach as a key direction for future research. This study did not address this. Second, to ensure a thorough assessment procedure, future research should consider additional selection criteria as well as other evolving dimensional models of MCS including individual, organizational, and policy actors. Future research can assess the feasibility of these alternatives. Third, risk management in MCS is dynamic by the development of the strategic environment, the research did not discuss the direction of risk management sustainability in the MCS dimension, future research can provide simulation-based sustainability analysis.

Acknowledgement

This research is supported by research from Indonesia Defense University. We also deliver our gratitude to maritime stakeholders who made important contributions to this research.

References

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

Akter, S., Debnath, B., & Bari, A. B. M. M. (2022). A grey decision-making trial and evaluation laboratory approach for evaluating the disruption risk factors in the Emergency Life-Saving Drugs supply chains. *Healthcare Analytics*, *2*(October), 100120. https://doi.org/10.1016/j.health.2022.100120

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, *45*(2019), 547–554. https://doi.org/10.1016/j.trpro.2020.03.058

Amirshenava, S., & Osanloo, M. (2018). Mine closure risk management: An integration of 3D risk model and MCDM techniques. *Journal of Cleaner Production*, *184*, 389–401. https://doi.org/10.1016/j.jclepro.2018.01.186

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. Bin, & Nosheen, S. (2022). A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Transactions on Intelligent Transportation Systems*, *24*(2), 2677–2690. https://doi.org/10.1109/TITS.2022.3164678

Biancini, A. (2016). 3PL provider selection by AHP and TOPSIS methodology. *Benchmarking: An International Journal*.

Bodeau, D. J., Graubart, R., & Fabius-Greene, J. (2010). Improving cyber security and mission assurance via cyber preparedness (cyber prep) levels. *Proceedings - SocialCom 2010: 2nd IEEE International Conference on Social Computing, PASSAT 2010: 2nd IEEE International Conference on Privacy, Security, Risk and Trust*, 1147–1152. https://doi.org/10.1109/SocialCom.2010.170

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. *Safety Science*, *131*. https://doi.org/10.1016/j.ssci.2020.104908

Boutkhoum, O., Hanine, M., Agouti, T., & Tikniouine, A. (2017). A decision-making approach based on fuzzy AHP-TOPSIS methodology for selecting the appropriate cloud solution to manage big data projects. *International Journal of System Assurance Engineering and Management*, *8*(s2), 1237–1253. https://doi.org/10.1007/s13198-017-0592-x

Bueger, C. (2015). What is maritime security? *Marine Policy*, *53*, 159–164. https://doi.org/10.1016/j.marpol.2014.12.005

Bueger, C., & Edmunds, T. (2020). Blue crime: Conceptualising transnational organised crime at sea. *Marine Policy*, *119*(January), 104067. https://doi.org/10.1016/j.marpol.2020.104067

Çalık, A., Çizmecioğlu, S., & Akpınar, A. (2019). An integrated AHP-TOPSIS framework for foreign direct investment in Turkey. *Journal of Multi-Criteria Decision Analysis*, *26*(5–6), 296–307. https://doi.org/10.1002/mcda.1692

Chang, C.-H., Kontovas, C., Yu, Q., & Yang, Z. (2021). Risk assessment of the operations of maritime autonomous surface ships. *Reliability Engineering and System Safety*, *207*. https://doi.org/10.1016/j.ress.2020.107324

Chapsos, I., & Malcolm, J. A. (2017). Maritime security in Indonesia: Towards a comprehensive agenda? *Marine Policy*, *76*(April 2016), 178–184. https://doi.org/10.1016/j.marpol.2016.11.033

Crotty, J., & Daniel, E. (2022). Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. *Applied Computing and Informatics*. https://doi.org/10.1108/ACI-07-2022-0178

Desiana, R., & Prima, S. C. (2022). Cyber security policy in Indonesian shipping safety. *Journal of Maritime Studies and National Integration*, *5*(2), 109–117. https://doi.org/10.14710/jmsni.v5i2.13673

Erdogan, M., & Kaya, I. (2019). Prioritizing failures by using hybrid multi criteria decision making methodology with a real case application. *Sustainable Cities and Society*, *45*(2019), 117–130. https://doi.org/10.1016/j.scs.2018.10.027

Erstad, E., Ostnes, R., & Lund, M. S. (2021). An operational approach to maritime cyber resilience. *TransNav*, *15*(1), 27–34. https://doi.org/10.12716/1001.15.01.01

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2017). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Analysis*, *9*. https://doi.org/10.1111/risa.12891

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

Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. *Computers and Security*, *103*. https://doi.org/10.1016/j.cose.2021.102196

Hareide, O. S., Josok, O., Lund, M. S., Ostnes, R., & Helkala, K. (2018). Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *Journal of Navigation*, *71*(5), 1025–1039. https://doi.org/10.1017/S0373463318000164

Haugli, M., Soldal, M., Larsen, M. H., Lund, M. S., & Bjørneseth, F. B. (2022). A model of factors influencing deck officers' cyber risk perception in offshore operations. *Maritime Transport Research*, *3*(March). https://doi.org/10.1016/j.martra.2022.100065

Hwang, C. L., & Yoon, K. (1981). *Multiple attribute decision making: Methods and applications.* Springer-Verlag. https://doi.org/10.1007/978-3-642-48318-9

Jiang, M., Liu, Y., Lu, J., Qu, Z., & Yang, Z. (2023). Risk assessment of maritime supply chains within the context of the Maritime Silk Road. *Ocean and Coastal Management*, *231*(September 2022), 106380. https://doi.org/10.1016/j.ocecoaman.2022.106380

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., & Chang, C. H. (2022). Maritime cybersecurity: are onboard systems ready? *Maritime Policy and Management*, *00*(00), 1–19. https://doi.org/10.1080/03088839.2022.2124464

Kechagias, E. P., Chatzistelios, G., & Papadopoulos, G. A. (2022). Digital transformation of the maritime industry : A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*, *37*(September 2021), 100526. https://doi.org/10.1016/j.ijcip.2022.100526

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences (Switzerland)*, *8*(6). https://doi.org/10.3390/app8060898

Larsen, M. H., & Lund, M. S. (2021). Cyber Risk Perception in the Maritime Domain : A Systematic Literature Review. *IEEE Access*, *9*, 144895–144905. https://doi.org/10.1109/ACCESS.2021.3122433

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2019). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors (Switzerland)*, *19*(1). https://doi.org/10.3390/s19010019

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

Marnani, C. S., Rumambi, F. J., & Simatupang, H. (2021). Analysis Of Connectivity Indonesia's Maritime Global Axis Policy With One World One Belt Road China Christine Sri Marnani, Freddy Johanes Rumambi, Haposan Simatupang. *Journal Online of Indonesian Defense University*, *1*(11).

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

Menon, R. R., & Ravi, V. (2022). Using AHP-TOPSIS methodologies in the selection of sustainable suppliers in an electronics supply chain. *Cleaner Materials*, *5*(February), 100130. https://doi.org/10.1016/j.clema.2022.100130

Mursitama, T. N., & Ying, Y. (2021). Indonesia's Perception and Strategy toward China's OBOR Expansion: Hedging with Balancing. *Chinese Economy*, *54*(1), 35–47. https://doi.org/10.1080/10971475.2020.1809816

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

Octavian, A., Widjayanto, J., Putra, I. N., Susilo, A. K., & Suharyo, O. S. (2020). Risk analysis of islamic state (Is) network development in southeast asia based on 3d matrix. *International Journal of Operations and Quantitative Management*, *26*(2), 195–223. https://doi.org/10.46970/2020.26.3.3

Park, C., Kontovas, C., Yang, Z., & Chang, C.-H. (2023). A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean and Coastal Management*, *235*. https://doi.org/10.1016/j.ocecoaman.2023.106480

Park, Changki, Shi, W., Zhang, W., Kontovas, C., & Chang, C. H. (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*, 79–86.

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber physical systems security for maritime assets. *Journal of Marine Science and Engineering*, *9*(12). https://doi.org/10.3390/jmse9121384

Putra, R. D., Supartono, & Deni, D. A. R. (2018). Ancaman Siber dalam Persfektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta). *Jurnal Prodi Perang Asimetris*, *4*(2), 99–120.

Rios Insua, D., Couce-Vieira, A., Rubio, J. A., Pieters, W., Labunets, K., & G. Rasines, D. (2021). An Adversarial Risk Analysis Framework for Cybersecurity. *Risk Analysis*, *41*(1), 16–36. https://doi.org/10.1111/risa.13331

Roege, P. E., Collier, Z. A., Chevardin, V., Chouinard, P., Florin, M. V., Lambert, J. H., Nielsen, K., Nogal, M., & Todorovic, B. (2017). Bridging the gap from cyber security to resilience. In *NATO Science for Peace and Security Series C: Environmental Security* (Vol. PartF1). https://doi.org/10.1007/978-94-024-1123-2_14

Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, *1*(1), 83–98. https://doi.org/10.1108/JMTM-03-2014-0020

Saini, S., & Singh, D. (2022). Reckoning with the barriers to Lean implementation in Northern Indian SMEs using the AHP-TOPSIS approach. *Journal of Science and Technology Policy Management*, *13*(3), 683–712. https://doi.org/10.1108/JSTPM-02-2020-0032

Sharma, M., & Sehrawat, R. (2020). A hybrid multi-criteria decision-making method for cloud adoption: Evidence from the healthcare sector. *Technology in Society*, *61*(April), 101258. https://doi.org/10.1016/j.techsoc.2020.101258

Singh, P. K., & Sarkar, P. (2019). A framework based on fuzzy AHP-TOPSIS for prioritizing solutions to overcome the barriers in the implementation of ecodesign practices in SMEs. *International Journal of Sustainable Development and World Ecology*, *26*(6), 506–521. https://doi.org/10.1080/13504509.2019.1605547

Solangi, Y. A., Tan, Q., Mirjat, N. H., Valasai, G. Das, Khan, M. W. A., & Ikram, M. (2019). An integrated Delphi-AHP and fuzzy TOPSIS approach toward ranking and selection of renewable energy resources in Pakistan. *Processes*, *7*(2), 1–31. https://doi.org/10.3390/pr7020118

Subagyo, A. (2018). Sinergi Dalam Menghadapi Ancaman Cyber Warfare. *Jurnal Pertahanan & Bela Negara*, *5*(1), 89–108. https://doi.org/10.33172/jpbh.v5i1.350

Susilo, A. K., Ciptomulyono, U., Putra, I. N., Ahmadi, & Suharyo, O. S. (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), 3–16.

Tissir, N., El Kafhali, S., & Aboutabit, N. (2021). Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. *Journal of Reliable Intelligent Environments*, *7*(2), 69–84. https://doi.org/10.1007/s40860-020-00115-0

Tseng, Y. P., Huang, Y. C., Li, M. S., & Jiang, Y. Z. (2022). Selecting Key Resilience Indicators for Indigenous Community Using Fuzzy Delphi Method. *Sustainability (Switzerland)*, *14*(4), 1–19. https://doi.org/10.3390/su14042018

Valis, D., & Koucky, M. (2009). Selected overview of risk assessment techniques. *Problemy Eksploatacji*, *4*, 19–32.

Yoo, Y., & Park, H. S. H.-S. H. S. (2021). Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. *Journal of Marine Science and Engineering*, *9*(6). https://doi.org/10.3390/jmse9060565