JOURNAL OF MARITIME RESEARCH

Vol XX. No. II (2023) pp 13–24

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

Cyber Threat Analysis of Maritime Cybersecurity Using AHP-Topsis

I Nengah Putra[1], A. Octavian[1], A.K. Heikhmakhtiar[1], Hendrana Tjahjadi[1], A.K. Susilo[2,*],

ARTICLE INFO

Article history:
Received 28 Feb 2023;
in revised from 13 Mar 2023;
accepted 30 Mar 2023.

Keywords:
Maritime Cybersecurity; Cyber Threat; Analytic Hierarchy Process (AHP); Technique For Order Preference By Similiarity To Ideal Solution (TOPSIS). .

ABSTRACT

This research aimed to provide an assessment of cyber threats to the maritime cybersecurity system in the Indonesian sea region. This research used the Analytic Hierarchy Process (AHP) and Technique for Order Preference By Similiarity To Ideal Solution (TOPSIS). AHP – TOPSIS is used to provide weight and comparison of threat values based on six maritime domain cyber threat criteria. Furthermore, cyber threats were identified based on five levels of cyber threats. Based on the research results, Human Factors (28.1%) were the most important criterion of the six evaluation components, followed by Man in the middle attack (MITM) (17%), Malware (16.2%), Outdated systems (15.4%), Phishing (15 %), and Thief of credentials (8.4%). The results of the evaluation of the threat level, Economics Fraud occupied the highest threat value of 0.628 with the Cyber Sabotage level category (Level 4). There were three threats included in the Cyber Incursion level (Level 3), including Value of cargo, Manipulation of signals used by ships, and IT-systems. Furthermore, six threats fell into the Cyber Theft category (Level 2), including Firewalls, Espionage on maritime operations, State-level threats, Misuse of AIS and data positioning, Insider threats, Computer Installations.

1. Introduction.

There is a long history of maritime operations and awareness of threats and consequences in purely physical space (Jones, Tam and Papadaki, 2016). In recent times, the industry has changed to a point where there is a heavy dependence on technology (Erstad, Ostnes and Lund, 2021). Innovative technologies have expanded into the marine transportation sector because they minimize costs and maximize profits in daily operations (Karamperidis, Kapalidis and Watson, 2021). The shift of the administration system at the port from a conventional administration system to digital has led to new risks, in the form of data theft vulnerabilities through cyber networks (Bolbot et al., 2022). Even though the maritime cyber domain is still relatively new, the resulting impact if cybercrime occurs in the maritime domain is very large (Karamperidis, Kapalidis and Watson, 2021).

Maritime cybersecurity is evolving as an issue affecting the oceans (Kanwal et al., 2022). In fact, over the past decade, there has been no major research focusing on maritime cybersecurity issues and ways to address them (You, Zhang and Cheng, 2017). As previously mentioned, there is awareness of maritime cybersecurity issues, but few are willing to study them because no major incidents have occurred to attract public attention (McGillivary, 2018; Kanwal et al., 2022). The field of maritime cybersecurity is almost empty and there is much that needs to be done quickly (You, Zhang and Cheng, 2017). Therefore, addressing maritime cybersecurity is a valid and important scientific research area for marine science (McGillivary, 2018; Bolbot et al., 2022).

However, not only is there very little data available, due to limited and evolving reporting capabilities, but cyber-maritime evolution makes the data unstable making it very difficult to develop reliable probabilities. This, in turn, makes it difficult to build a qualitative maritime cyber risk assessment in the maritime field (Kimberly Tam and Jones, 2019). Bolbot et al. (2022), explained the need to develop research proposals, new methodologies and technical solutions and in general will promote maritime cybersecurity. While Larsen et al. (2022), explained the

[1] Indonesia Defense University, Sentul-Sukahati, Citeureup-Bogor, Indonesia.

[2] Airlangga University, Airlangga-Gubeng, Surabaya, East-Java, Indonesia.

[*] Corresponding author: A.K. Susilo. E-mail Address: april.kukuh.susilo-2020@feb.unair.ac.id.

need for decision-makers to address the potential for severe cyber incidents in the maritime transportation system. Meland et al. (2021), suggested the need to develop knowledge about fragmented incidents and threats in maritime cyber. You et al., (2017), also suggested future studies on maritime cybersecurity assessment and evaluation. Therefore, it is necessary to analyze the value of cyber threats in the maritime domain in the Indonesian sea area.

This research aimed to provide an assessment of cyber threats to the maritime cybersecurity system in the Indonesian Sea region. In Indonesia, there are still few Maritime Cyber Security policies and socialization of security guarantees within government agencies. This needs to be a priority for the government, considering the sophistication of technology which is increasing every year and the increasing vulnerability to cyber threats (Desiana and Prima, 2022). Technological developments in the maritime sector provide efficiency to environmental operations. The development of evaluation and measurement of maritime cybersecurity threats into research is the main attraction of this research. The development of analytical insights about maritime cyber security threats which are still limited provides another side on aspects of cyber risk that can complement the existing literature review.

This research used AHP and TOPSIS to identify and analyze cyber threats in the maritime cyber security domain in the Indonesian seas. The qualitative descriptive statistical method approach was chosen with the consideration of building an assessment of maritime cyber threat analysis as recommended by Tam & Jones (2019). AHP – TOPSIS is used to provide weight and comparison of threat values based on six maritime domain cyber threat criteria. Furthermore, cyber threats are identified based on five levels of cyber threats.

There are several contributions offered in this research. This study fills the gaps in qualitative analysis on cyber threat aspects in the maritime domain. Second, this research enriches the literature on handling maritime cyber security in marine science. Third, this research can provide an evaluation framework for maritime cyber threats in reducing the risk of incidents occurring in the maritime area. Fourth, the development of existing research literature, methodologies and theories as well as technical solutions in promoting maritime cybersecurity threats is an additional contribution.

This research consists of several parts. Section 2 provides an explanation regarding the literature review, including Maritime Cyber and Cyber threats. Section 3 describes the methodology which consists of research design, Conceptual framework, Analytical Hierarchy Process (AHP) Method, TOPSIS method. Section 4 describes the results and discussion, including determining criteria and alternatives for threats, weighting criteria and analysis of threat levels, sensitivity analysis. Section 5 is the conclusion of the research, implications, research limitations and future research.

2. Literature Review.

2.1. Maritime Cyber.

The 21st-century maritime cyber threat environment requires a broader scope and a more comprehensive vision. Decision advantage is made possible by ensuring global maritime information dominance through the collection, integration and dissemination of information and intelligence, and knowledge development. This requires stronger partnerships and information sharing on security plans, cyber risk and cyber mitigation with all components of the maritime sector (including government agencies, port facilities, ship owners and operators) and the technical community that supports maritime infrastructure (Greiman, 2020).

Information technology is rapidly becoming a component of the maritime space, the port and shipping sector will fully rely on it in the future. However, with this digital transition comes new dangers that could jeopardize the effectiveness of these systems. As the economy and global transportation networks are interrelated and widely connected, the impact of maritime cybersecurity threats may harm stability in the region (Tam & Jones, 2019). A recent maritime cybersecurity incident revealed that shipping is facing increased exposure to cyber threats, especially due to the rapidly growing digitization of this sector, leaving ships and the systems within them vulnerable to cyberattacks (Kanwal et al., 2022). Understanding maritime cyber threats is a challenge because threats can be complex and evolving risks that affect trade, geopolitics, and security (Kuhn, Bicakci and Shaikh, 2021).

In the aspect of maritime cyber threats, maritime cyber risk has been defined as a measure of the extent to which a technology asset is threatened by potential circumstances or events, which may result in operational, safety, or shipping-related security failures as a consequence of damaged, lost or compromised information or systems (Park et al., 2019). Because cybersecurity vendors often only consider the technological part of the maritime environment, it is very important to remember that one part of the system cannot be viewed in isolation, but must be seen about other parts (Erstad, Ostnes and Lund, 2021). Thus, maritime cyber threats here are understood as cyber threats that affect the maritime domain (Erstad, Ostnes and Lund, 2021). The maritime cyber threat landscape shows that malware infection is a common way to compromise systems, the scope of the assessment on the adverse events in which one or several sub-components may be infected and the probabilities associated (Meland et al., 2022).

2.2. Cyber threat.

A cyber threat is any occurrence that has the potential to adversely affect a person, property (tangible or intangible), organization or country by unauthorized access through an information system. Cyberattacks can be targeted on any device connected to the internet with the malicious aim of disrupting or damaging and society's dependence on digital technology will create more opportunities for cyberattacks (Seetharaman et al., 2021). Cyber threats are one of the main risks facing companies today and affect most companies every year (Carías et al., 2020). However, the most organic solution is to provide the information resources themselves with suitable functionality, which will ensure their protection while taking into account the specific operating conditions. The solution to this problem involves considering the cyber threats that must be resisted by the protection system and the specific features of the protected information resources (Luskatov and Pilkevich, 2019).

Cyber threats are multifaceted and rapidly evolving. Impact assessment and risk management are important parts of evaluating cyber situations and offering remediation as part of a mitigation plan (Steingartner and Galinec, 2021). Cyberthreats are constantly exploiting the connectivity and complexity in critical infrastructure to plan and launch attacks against existing computer systems. This is a big challenge experienced by various business organizations. (Fakiha, 2020).

3. Methodology.

This research was conducted in the maritime field, especially cybersecurity which is located in the Indonesian Sea region. The main purpose of this research was to evaluate and provide a cyber threat level value to the field of maritime cybersecurity. Questions related to threat identification were framed on a five-point Likert scale ranging from 1 to 5 in Table 2. 18 experts were selected as Tseng et al. (2022), related to the cyber-maritime field through purposive sampling contacted via email and google forms (Akter, Debnath and Bari, 2022; Bari et al., 2022) for data collection. Most of the experts in this research were 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 competency. Their opinions and suggestions helped the author build a threat hierarchy and improve the questionnaire.

3.1. Conceptual framework.

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

- Identifying criteria and alternative types of threats to Maritime Cybersecurity;
- Analyzing and measuring the level of threats to Maritime Cybersecurity using the AHP-TOPSIS approach;
- Validating results and models using sensitivity analysis.

This research also developed a model that is able to provide an assessment and measurement of threat levels against Maritime Cybersecurity. The proposed model considered the prequalification process during the planning stage. It should be noted that the TOPSIS and AHP techniques were used due to their several advantages, as were Marzouk & Sabbah (2021) and Saini & Singh (2022). The model mechanism illustrated in the flowchart shown in Figure 1 was divided into three modification phases by Menon & Ravi (2022) and Boutkhoum et al. (2017).

Phase 1 – This article considered the threat assessment in maritime cybersecurity, determined the criteria, and types of threats through a literature review and discussion with experts to generate an idea about all the criteria that need to be considered when making a decision. This stage ended when a consensus on the criteria and types of cyber threats had been reached.

Phase 2 – The script's approach considered six main criteria. Through literature review and expert opinion, these criteria were identified. Questionnaires were given to get responses in identifying criteria and producing a hierarchical structure and followed by calculating the relative importance/weight of these criteria.

Phase 3 – Analysis of threats to maritime cybersecurity was evaluated based on parameters against criteria. TOPSIS was adopted to rank and measure threat-level values in the decision-making process. At the end of this process, a sensitivity analysis was carried out to measure the effect of the weighting of the criteria on the final decision-making process.

3.2. Analytical Hierarchy Process (AHP) Method.

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:

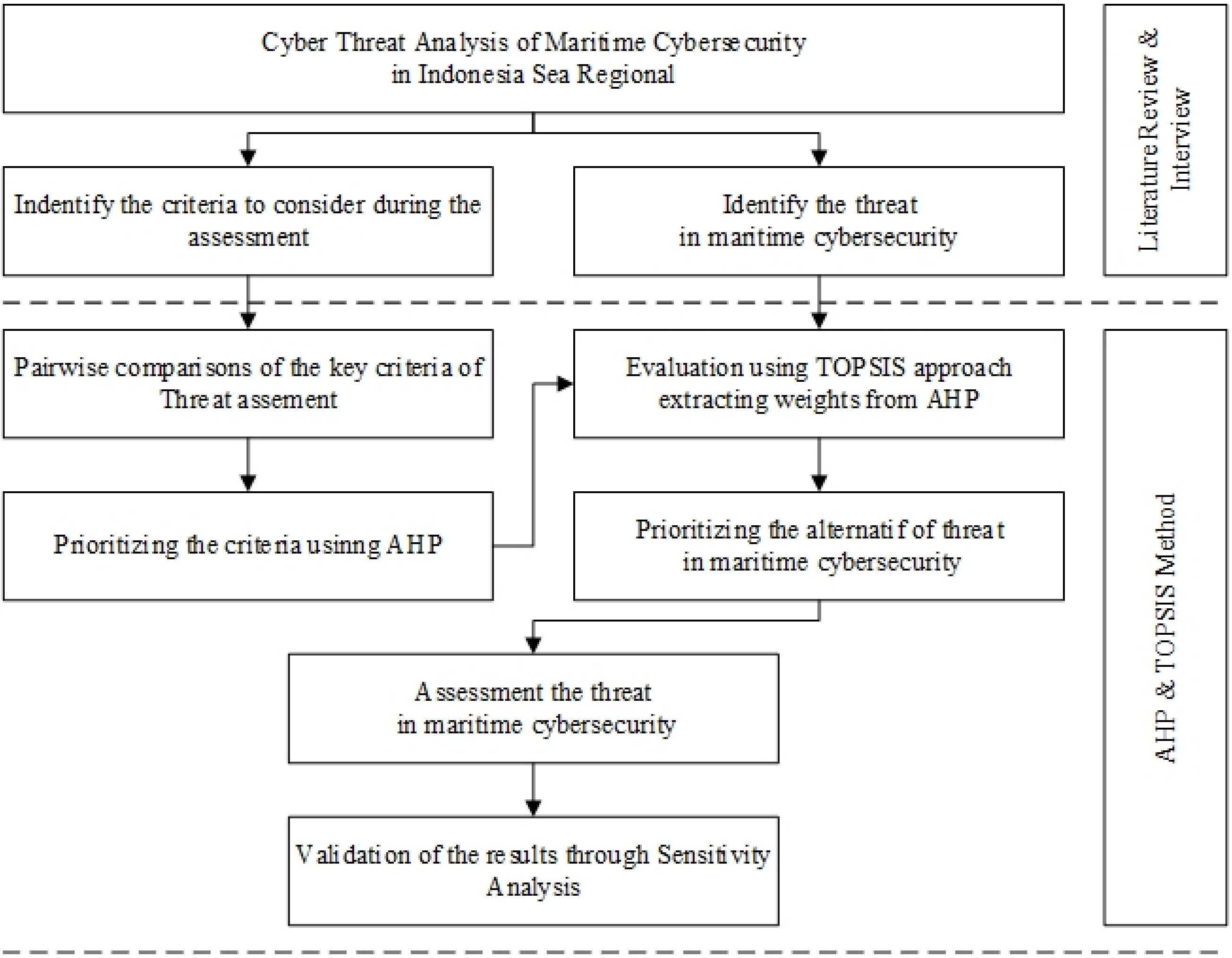
- The purpose of the problem is defined.
- The decision hierarchy framework is drawn according to the alternatives.
- Pairwise comparisons of criteria are made, and pairwise comparison matrices are developed.
- Benchmark weights are obtained from the pairwise comparison matrix.
- Consistency of specified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

Figure 1: Conceptual framework of Threat Analysis in Maritime Cybersecurity.


Cyber Threat Analysis of Maritime Cybersecurity in Indonesia Sea Regional
Indentify the criteria to consider during the assessment
Identify the threat in maritime cybersecurity
Literature Review & Interview
Pairwise comparisons of the key criteria of Threat assement
Evaluation using TOPSIS approach extracting weights from AHP
Prioritizing the criteria usinng AHP
Prioritizing the alternatif of threat in maritime cybersecurity
Assessment the threat in maritime cybersecurity
Validation of the results through Sensitivity Analysis
AHP & TOPSIS Method

Source: Modified from Afrane et al. (2022); Saini & Singh (2022); Solangi et al. (2019).

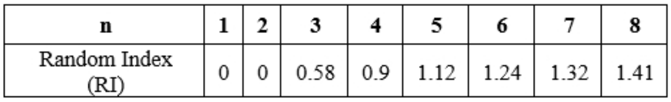
$$CI = \frac{\lambda_{max} - n}{n}; \quad (1)$$

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

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

$$CR = \frac{CI}{RI}; \quad (2)$$

Table 1: 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 and W's 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.

3.3. TOPSIS method.

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, Çizmecioğlu and Akpınar, 2019).

a. Creating a matrix of Cyber threat Analysis decision-making.
b. Normalizing the decision matrix.

$$X = \begin{bmatrix} X_{11} & X_{12} & ... & X_{1n} \\ X_{21} & X_{22} & ... & X_{2n} \\ ... & ... & ... & ... \\ X_{m1} & X_{m2} & ... & X_{mn} \end{bmatrix} \tag{3}$$

$$r_{ij} = \frac{X_{ij}}{\sqrt{\sum_{k=1}^{m} X_{kj}^2}} \tag{4}$$

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

$$y_{ij} = w_j xrij; \tag{5}$$

where: i = 1,2,3,..m; j=1,2,3,..n

$$Y = \begin{bmatrix} w_1 & w_2 & ...w_m \end{bmatrix} \begin{bmatrix} r_{11} & r_{12} & .. & r_{1n} \\ r_{21} & r_{22} & .. & r_{2n} \\ .. & .. & .. & .. \\ r_{m1} & r_{m2} & .. & r_{mn} \end{bmatrix} =$$

$$= \begin{bmatrix} w_1 r_{11} & w_2 r_{12} & .. & w_n r_{1n} \\ w_1 r_{21} & w_2 r_{22} & .. & w_n r_{2n} \\ .. & .. & .. & .. \\ w_1 r_{m1} & w_2 r_{m2} & .. & w_n r_{mn} \end{bmatrix} \tag{6}$$

d. Determining a positive ideal solution matrix and a negative ideal solution matrix (Nazam, et al., 2015).

$$A^+ = (y_1^+, y_2^+, ..., y_n^+); A^- = (y_1^-, y_2^-, ..., y_n^-) \tag{7}$$

Based on normalized weight, the positive ideal solution A^+ and the ideal solution A^- may be established (y_{ij}). 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 (y_{ij}). 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 and Kaya, 2019).

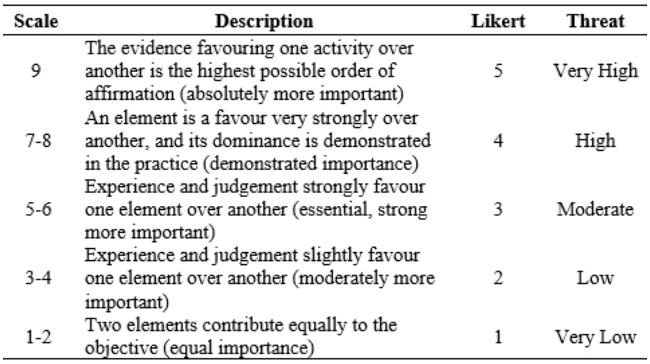
$$D_i^+ = \sqrt{\sum_{j=i}^{n}((y_{ij} - y_j^+)^2)} \;\&\; D_i^- = \sqrt{\sum_{j=i}^{n}((y_{ij} - y_j^-)^2)} \tag{8}$$

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

$$V_i = \frac{D_i^-}{D_i^- + D_i^+} \tag{9}$$

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

Table 2: Scale of pairwise comparison for AHP and likert scale for TOPSIS.



Scale	Description	Likert	Threat
9	The evidence favouring one activity over another is the highest possible order of affirmation (absolutely more important)	5	Very High
7-8	An element is a favour very strongly over another, and its dominance is demonstrated in the practice (demonstrated importance)	4	High
5-6	Experience and judgement strongly favour one element over another (essential, strong more important)	3	Moderate
3-4	Experience and judgement slightly favour 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).

4. Results & Discussion.

4.1. Determination of criteria and alternatives to threats.

In the first stage of application, evaluation criteria and alternatives had to be determined, and a hierarchical structure of the problem had to be defined. Identification of criteria in threat analysis on maritime cybersecurity included input in the form of previous studies supported by expert opinion for alternative data and processes including the stages of the AHP and TOPSIS methods, and output in the form of evaluating the value of threats to maritime cybersecurity in Indonesia's maritime territory.

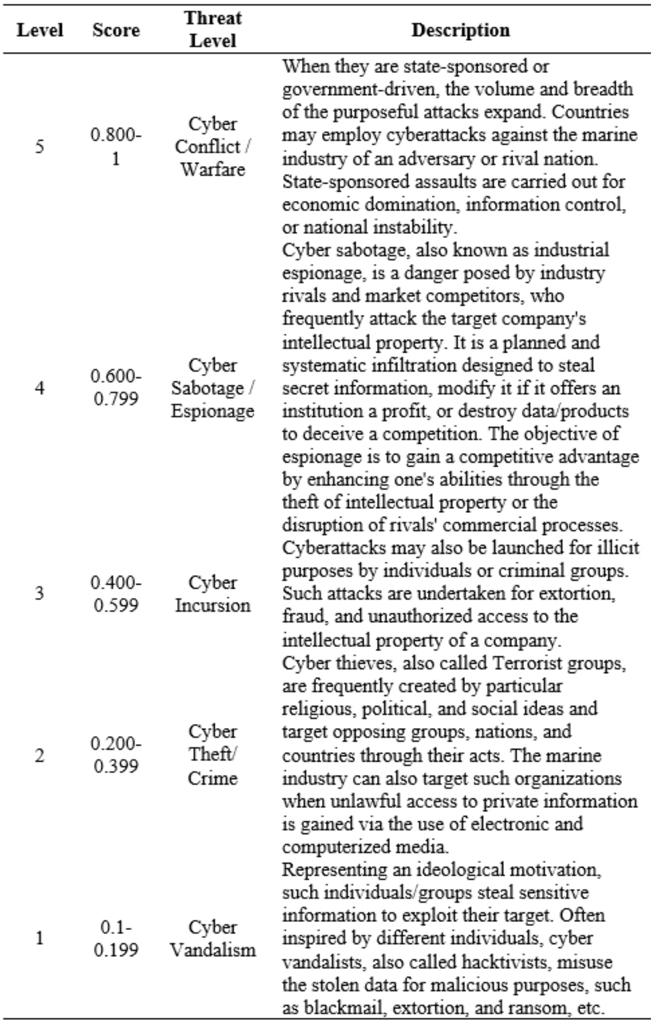
18 different experts (academicians, maritime security experts, and cyber threat experts) were surveyed to determine the importance of the criteria. According to the survey results, criteria with a high total score form an input hierarchy entry that will be used in the identification of criteria. All the criteria that affect the decision on the value of threats in maritime cybersecurity are determined by experts. Maritime cyber threat criteria have been developed, based on preliminary technical studies and surveys from Ashraf et al. (2022); Kanwal et al. (2022); C Park et al. (2023) which is applied in the field of maritime cybersecurity. Therefore, the final list includes six main criteria including a) Phishing; b) Malware; c) Man in the middle attack; d) Thief of credentials; e) Human factors; f) outdated systems.

a. Phishing (C1).

Phishing refers to the act of sending emails that appear to be impersonated and contain links to fake websites or malicious files or text messages (Park et al., 2023). Phishing attacks involving e-mail malware impersonate ship operators, who send it to ships via e-mail attachments (Kuhn, Bicakci and Shaikh, 2021). The email may appear to have been sent by a bank or other law firm. Marine personnel using personal devices can create cybersecurity difficulties by receiving phishing emails or visiting malicious websites, thereby infecting the ship's operational systems with harmful viruses (Akpan et al., 2022).

b. Malware (C2).

Table 3: Threat Level of Maritime Cybersecurity.



Level	Score	Threat Level	Description
5	0.800-1	Cyber Conflict / Warfare	When they are state-sponsored or government-driven, the volume and breadth of the purposeful attacks expand. Countries may employ cyberattacks against the marine industry of an adversary or rival nation. State-sponsored assaults are carried out for economic domination, information control, or national instability.
4	0.600-0.799	Cyber Sabotage / Espionage	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. It is a planned and systematic infiltration designed to steal secret information, modify it if it offers an institution a profit, or destroy data/products to deceive a competition. The objective of espionage is to gain a competitive advantage by enhancing one's abilities through the theft of intellectual property or the disruption of rivals' commercial processes.
3	0.400-0.599	Cyber Incursion	Cyberattacks may also be launched for illicit purposes by individuals or criminal groups. Such attacks are undertaken for extortion, fraud, and unauthorized access to the intellectual property of a company.
2	0.200-0.399	Cyber Theft/ Crime	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. The marine industry can also target such organizations when unlawful access to private information is gained via the use of electronic and computerized media.
1	0.1-0.199	Cyber Vandalism	Representing an ideological motivation, such individuals/groups steal sensitive information to exploit their target. Often inspired by different individuals, cyber vandalists, also called hacktivists, misuse the stolen data for malicious purposes, such as blackmail, extortion, and ransom, etc.

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

Malware is malicious software that evaluates or damages the system without the user’s knowledge and spreads through downloading files attached to infected emails, visiting fraudulent websites, or connecting USB drives and portable media that carry malware (Amro and Gkioulos, 2023). This condition results in ransomware or Distributed Denial of Service (DDoS) attacks (Ben Farah et al., 2022). Between 2010 and 2020, Meland et al. (2021), described several marine hacks caused by malware. Mrakovi’c and Vojinovi’c (2019) noted that malware is one of the most common forms of cyberattacks in the marine industry (2020) and asserted that malware is the top choice for bad actors to compromise maritime cybersecurity.

c. Man in the middle attack (MITM) (C3).

A type of malware that relies on weaknesses in the SSL/TLS protocol, being a correspondent in communication between two network users (Mraković and Vojinović, 2019). Through man-in-the-middle attacks, hackers can eavesdrop on any communications between parties and/or impersonate them. Hackers hide their presence on free/open WiFi hotspots or fake websites and restrict users from sending and receiving data, or even redirecting data to other users (Suciu et al., 2019). In the maritime field, this type of cyber threat often targets remote desktop protocol (RDP) services operating on Electronic Chart Information and Display Systems (ECDIS) (Svilicic et al., 2019). The attacker then tries to perform the “Man-in-the-Middle: ARP Cache Poisoning” technique to be able to “Network Sniffing” of the traffic (Amro and Gkioulos, 2023).

d. Thief of credentials (C4).

Credential theft is a kind of cyber hazard that requires stealing identity proof from users or customers (Park et al., 2023). Hackers can easily exploit insecure authentication methods and weak passwords (Akpan et al., 2022). When the ECDIS application is running under administrative credentials, remote vulnerability scanning is performed without administrative privileges (Svilicic et al., 2019). Security uses a public/private key encryption method with key access, everyone who tries to breach the system will face authentication through a secure credential system to access the system’s operational resources over the network (Ding et al., 2022).

e. Human factor (C5).

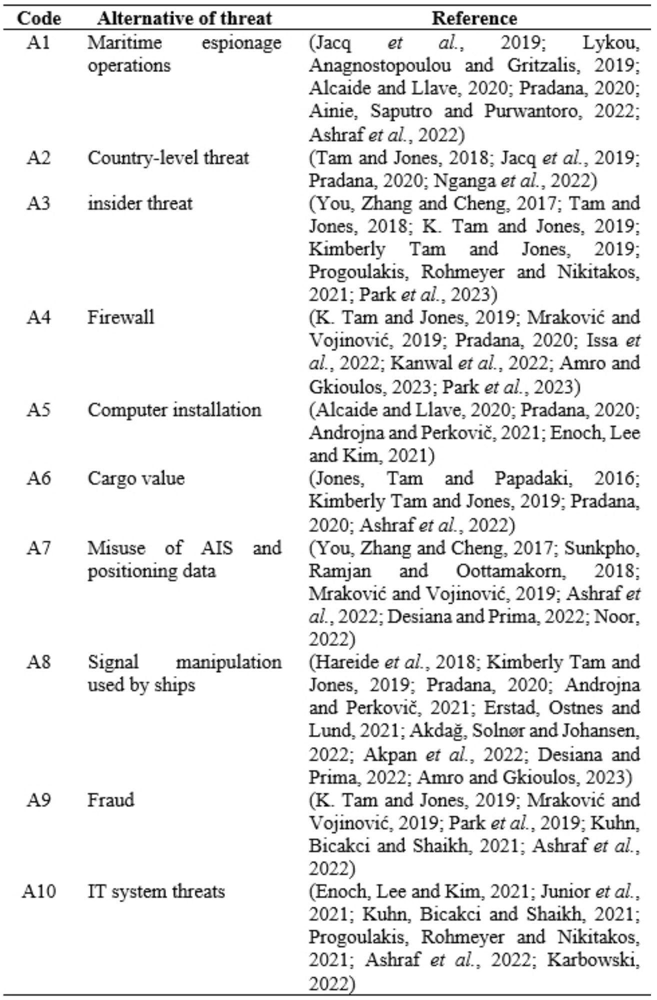
80–90% of maritime safety and security problems are directly or indirectly caused by human error, which has been identified as a major element (Chang et al., 2021). On the other hand, there is also an insider threat, meaning that someone within the organization can damage it for personal gain or special reasons, such as stealing sensitive information (Park et al., 2023). Indeed, the human factor is seen as the greatest danger to maritime cybersecurity (Tusher et al., 2022). The technological growth of the marine sector has increased the number of unwanted human errors that expose the maritime industry to cyber-attacks (Tam et al., 2023). Some human errors related to cybersecurity can be associated with any of the following activities such as accessing suspicious websites or links or disabling firewalls through carelessness or for some purpose, using personal devices on ship systems (Kanwal et al., 2022). It is important to consider that the human factor plays a fundamental role in the effectiveness of cyber attacks as a significant element of vulnerability for companies (Alcaide and Llave, 2020)

f. Outdated systems (C6).

Maritime cybersecurity vulnerabilities found that shipping companies rely too heavily on outdated technologies and use outdated versions of antivirus software, which poses significant harm (Kanwal et al., 2022). Without up-to-date IT infrastructure, hackers can target ships or businesses with viruses or malware, which are difficult to detect and protect against using conventional antivirus software (Park et al., 2019; Ben Farah et al. 2022; Tusher et al., 2022). Outdated software systems also pose a real cybersecurity risk and lack of timely application of patches/updates can also make current systems vulnerable (Kanwal et al., 2022). In addition, many ships continue to use outdated systems (e.g., old software) that are no longer supported by the software vendor, and these systems may have software vulnerabilities that security administrators are not aware of (Enoch, Lee and Kim, 2021).

After the evaluation criteria are determined, there are ten main cyber-attack models, including a) Maritime operational espionage; b) country-level threats; c) insider threats; d) firewalls; e) Computer installation; f) the value of the cargo; g) Misuse of AIS and positioning data; h) Manipulation of signals used by ships; i) Fraud; j) threats to IT systems. Then evaluated according to the proposed methodology.

Table 4: Ten models of cyber threats in maritime cyber security.



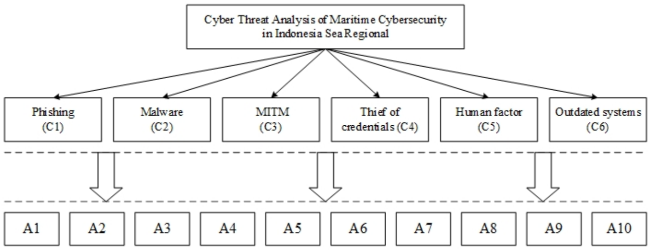
Code	Alternative of threat	Reference
A1	Maritime espionage operations	(Jacq *et al.*, 2019; Lykou, Anagnostopoulou and Gritzalis, 2019; Alcaide and Llave, 2020; Pradana, 2020; Ainie, Saputro and Purwantoro, 2022; Ashraf *et al.*, 2022)
A2	Country-level threat	(Tam and Jones, 2018; Jacq *et al.*, 2019; Pradana, 2020; Nganga *et al.*, 2022)
A3	insider threat	(You, Zhang and Cheng, 2017; Tam and Jones, 2018; K. Tam and Jones, 2019; Kimberly Tam and Jones, 2019; Progoulakis, Rohmeyer and Nikitakos, 2021; Park *et al.*, 2023)
A4	Firewall	(K. Tam and Jones, 2019; Mraković and Vojinović, 2019; Pradana, 2020; Issa *et al.*, 2022; Kanwal *et al.*, 2022; Amro and Gkioulos, 2023; Park *et al.*, 2023)
A5	Computer installation	(Alcaide and Llave, 2020; Pradana, 2020; Androjna and Perkovič, 2021; Enoch, Lee and Kim, 2021)
A6	Cargo value	(Jones, Tam and Papadaki, 2016; Kimberly Tam and Jones, 2019; Pradana, 2020; Ashraf *et al.*, 2022)
A7	Misuse of AIS and positioning data	(You, Zhang and Cheng, 2017; Sunkpho, Ramjan and Oottamakorn, 2018; Mraković and Vojinović, 2019; Ashraf *et al.*, 2022; Desiana and Prima, 2022; Noor, 2022)
A8	Signal manipulation used by ships	(Hareide *et al.*, 2018; Kimberly Tam and Jones, 2019; Pradana, 2020; Androjna and Perkovič, 2021; Erstad, Ostnes and Lund, 2021; Akdağ, Solnør and Johansen, 2022; Akpan *et al.*, 2022; Desiana and Prima, 2022; Amro and Gkioulos, 2023)
A9	Fraud	(K. Tam and Jones, 2019; Mraković and Vojinović, 2019; Park *et al.*, 2019; Kuhn, Bicakci and Shaikh, 2021; Ashraf *et al.*, 2022)
A10	IT system threats	(Enoch, Lee and Kim, 2021; Junior *et al.*, 2021; Kuhn, Bicakci and Shaikh, 2021; Progoulakis, Rohmeyer and Nikitakos, 2021; Ashraf *et al.*, 2022; Karbowski, 2022)

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

4.2. Criteria weighting and Threat level analysis.

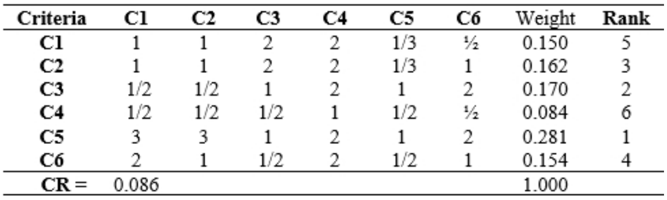
As seen in Figure 2, the hierarchical structure of the problem has been built based on the main and alternative criteria. After using expert opinion to develop selection criteria, MS Excel application was used to complete the approach. After the preparatory phase, a group of six professionals (academicians, maritime experts and cyber experts) reviewed the criteria and alternatives. The significance of the criteria was determined using the linguistic factors presented in Table 4. The level of significance of the criteria was determined using the AHP technique and Table 5 by applying a combined evaluation of the criteria.

Figure 2: The hierarchical analysis structure of the study.


Cyber Threat Analysis of Maritime Cybersecurity in Indonesia Sea Regional
Phishing (C1)
Malware (C2)
MITM (C3)
Thief of credentials (C4)
Human factor (C5)
Outdated systems (C6)
A1
A2
A3
A4
A5
A6
A7
A8
A9
A10

Source: Authors.

Table 5: Combined paired comparison matrix for criteria.



Criteria	C1	C2	C3	C4	C5	C6	Weight	Rank
C1	1	1	2	2	1/3	½	0.150	5
C2	1	1	2	2	1/3	1	0.162	3
C3	1/2	1/2	1	2	1	2	0.170	2
C4	1/2	1/2	1/2	1	1/2	½	0.084	6
C5	3	3	1	2	1	2	0.281	1
C6	2	1	1/2	2	1/2	1	0.154	4
CR =	0.086						1.000	

After compiling the section on the importance of key factors influencing a valid questionnaire, C.I. value 0.107 and value of C.R. was 0.086 for the six assessment criteria. This showed that a valid questionnaire met the consistency standard. The relative importance of the key factors influencing threats to maritime cybersecurity was shown in Table 5. Among the six criteria, Human Factors (28.1%) was the most important criterion of the six evaluation components, followed by Man in the middle attack (MITM) (17 %), Malware (16.2%), Outdated systems (15.4%), Phishing (15%), and Thief of credentials (8.4%).

Human factors could create risks where technology and humans interact and could generate major risk challenges including aspects of personnel vulnerability associated with human operators across systems and process architectures (Progoulakis, Rohmeyer and Nikitakos, 2021). It was important to consider that the human factor played a fundamental role in the effectiveness of cyber-attacks as a significant element of vulnerability (Alcaide and Llave, 2020). Human factor threats consist of unintentional security breaches, use of infected information media accidentally providing sensitive information, and lack of awareness and human error (Kure, Islam and Razzaque, 2018).

Next, determine the weighting of the evaluation criteria, using the weight of the alternative threat criteria that were analyzed using the TOPSIS method and determined and evaluated the value of the threat level that occurs in maritime cybersecurity with the positive ideal solution and the farthest from the negative ideal solution, which was most appropriate in priority order and displayed in Table 6. At this stage, the decision-making group gave a score of between 1 and 5 points for the specified list of threats. The decision matrices collected in Table 7 were obtained for the data, which were evaluated by the experts for the threat. The values are given in Table 8 of the normalized values, and the normalized decision matrices.

Table 6: Aggregated decision evaluation matrix.

Weight	0.150	0.162	0.170	0.084	0.281	0.154
alternative / criteria	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**
M1	2.881	2.766	2.896	2.766	3.194	3.965
M2	2.734	2.965	2.896	3.366	3.104	3.965
M3	3.088	2.766	3.104	2.814	3.178	4.156
M4	3.178	2.551	2.656	2.881	3.178	4.156
M5	3.178	2.930	3.270	2.881	3.178	3.877
M6	3.088	3.000	2.670	2.766	2.521	4.443
M7	3.270	2.766	3.051	3.016	2.881	4.514
M8	3.088	2.766	2.881	3.016	3.051	3.314
M9	2.930	3.140	2.656	2.285	2.896	2.993
M10	3.194	3.016	2.896	2.847	2.896	3.758

Table 7: Normalized decision matrix.

alternative / criteria	C1	C2	C3	C4	C5	C6
M1	0.297	0.305	0.315	0.304	0.335	0.318
M2	0.282	0.327	0.315	0.370	0.326	0.318
M3	0.318	0.305	0.338	0.309	0.333	0.334
M4	0.328	0.281	0.289	0.317	0.333	0.334
M5	0.328	0.323	0.356	0.317	0.333	0.311
M6	0.318	0.330	0.291	0.304	0.264	0.357
M7	0.337	0.305	0.332	0.332	0.302	0.362
M8	0.318	0.305	0.314	0.332	0.320	0.266
M9	0.302	0.346	0.289	0.251	0.304	0.240
M10	0.329	0.332	0.315	0.313	0.304	0.302

Table 8 showed that among the six threat evaluations, Economics Fraud occupied the highest threat value of 0.628 with the Cyber Sabotage level category (Level 4) in the order of M9, M6, M8, M10, M4, M1, M2, M7, M3, and M5. Cyber-attacks could be aimed exclusively at stealing identities so they could be used for further crimes (Jones, Tam and Papadaki, 2016). Identity fraud that impacted the economy was generally carried out using malware (Mraković and Vojinović, 2019).

There were three threats included in the Cyber Incursion level (Level 3), namely Value of cargo, Manipulation of signals used by ships, IT-systems with respective coefficients of 0.532, 0.495 and 0.445. Furthermore, six threats fall into the Cyber Theft category (Level 2), namely Firewalls (0.395), Espionage on maritime operations (0.369), State-level threat (0.351), Misuse of AIS and positioning data (0.329), Insider threat (0.279), Computer Installations (0.267).

Table 8: Evaluation value of alternative maritime cybersecurity threat level.

Alternative	D+	D-	Result	Rank	Level
Espionage on maritime operations	0.024	0.014	0.369	6	Cyber Theft
State-level threat	0.025	0.013	0.351	7	Cyber Theft
Insider threat	0.027	0.010	0.279	9	Cyber Theft
Firewalls	0.026	0.017	0.395	5	Cyber Theft
Computer Installations	0.027	0.010	0.267	10	Cyber Theft
Value of cargo	0.021	0.024	0.532	2	Cyber Incursion
Misuse of AIS and positioning data	0.025	0.013	0.329	8	Cyber Theft
Manipulation of signals used by ships	0.019	0.019	0.495	3	Cyber Incursion
Economic fraud	0.016	0.026	0.628	1	Cyber Sabotage
IT-systems	0.019	0.016	0.445	4	Cyber Incursion
	Average Level		**0.409**		**Cyber Theft**

4.3. Sensitivity analysis.

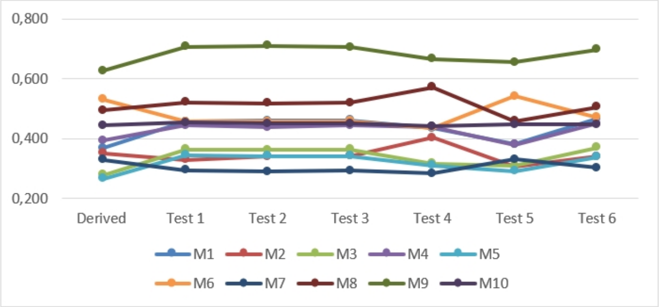
Sensitivity analysis is the study of how the uncertainty in the output of a model or mathematical system (numeric or otherwise) could be divided among the various sources of uncertainty in its input. Uncertainty analysis, which focused more on measuring uncertainty and the spread of uncertainty, was a similar technique. Optimally, the evaluation of uncertainty and sensitivity should be carried out simultaneously. Under sensitivity analysis, the process of recalculation of results based on different assumptions to identify the effect of a variable can serve a variety of purposes. The main objective is to evaluate the robustness of the model under conditions of uncertainty (Saini and Singh, 2022).

Different scenarios are investigated by keeping the weight of one criterion as a derivative, while the other criteria are given the same weight in Table 9. Scenarios with changing weights are checked for deviations from the original results. In the first scenario, the weight of the Phishing criteria is maintained, while the other five criteria are given the same weight.

Table 9: Evaluation value of alternative maritime cybersecurity threat level.

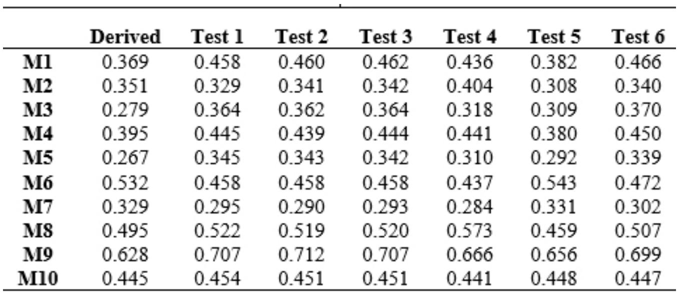
	Derived	Test 1	Test 2	Test 3	Test 4	Test 5	Test 6
C1	0.150	0.150	0.170	0.170	0.170	0.170	0.170
C2	0.162	0.168	0.162	0.168	0.168	0.168	0.168
C3	0.170	0.166	0.166	0.170	0.166	0.166	0.166
C4	0.084	0.183	0.183	0.183	0.084	0.183	0.183
C5	0.281	0.144	0.144	0.144	0.144	0.281	0.144
C6	0.154	0.169	0.169	0.169	0.169	0.169	0.154

Figure 3: Result of sensitivity analysis.



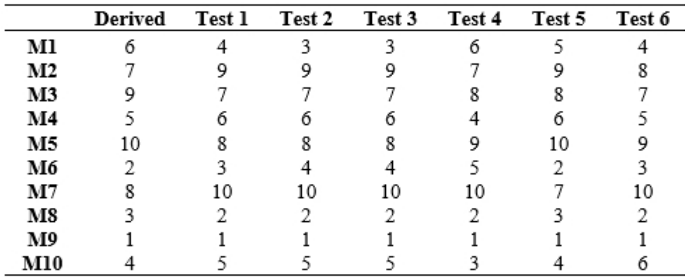
Source: Authors.

Table 10: Relative closeness values are obtained by different tests.



	Derived	Test 1	Test 2	Test 3	Test 4	Test 5	Test 6
M1	0.369	0.458	0.460	0.462	0.436	0.382	0.466
M2	0.351	0.329	0.341	0.342	0.404	0.308	0.340
M3	0.279	0.364	0.362	0.364	0.318	0.309	0.370
M4	0.395	0.445	0.439	0.444	0.441	0.380	0.450
M5	0.267	0.345	0.343	0.342	0.310	0.292	0.339
M6	0.532	0.458	0.458	0.458	0.437	0.543	0.472
M7	0.329	0.295	0.290	0.293	0.284	0.331	0.302
M8	0.495	0.522	0.519	0.520	0.573	0.459	0.507
M9	0.628	0.707	0.712	0.707	0.666	0.656	0.699
M10	0.445	0.454	0.451	0.451	0.441	0.448	0.447

Table 11: Rating of threat values from the results of sensitivity analysis testing.



	Derived	Test 1	Test 2	Test 3	Test 4	Test 5	Test 6
M1	6	4	3	3	6	5	4
M2	7	9	9	9	7	9	8
M3	9	7	7	7	8	8	7
M4	5	6	6	6	4	6	5
M5	10	8	8	8	9	10	9
M6	2	3	4	4	5	2	3
M7	8	10	10	10	10	7	10
M8	3	2	2	2	2	3	2
M9	1	1	1	1	1	1	1
M10	4	5	5	5	3	4	6

The threat evaluation ratings were found in the order of M9, M6, M8, M10, M4, M1, M2, M7, M3, and M5. Likewise, scenarios were changed by considering the actual weight of one criterion and giving the same weight to other criteria. The assigned weights were shown Table 9. The relative closeness values obtained in the different scenarios were shown in Table 10. The results of the sensitivity analysis were shown in Figure 3. The variation in the threat evaluation under different scenarios in the sensitivity analysis was shown in Table 11. It was seen that there was no large variation in ranking order under different scenarios, and M9 is the most powerful maritime cybersecurity aspect cyber threat. Thus, the proposed model is robust.

Conclusions.

In Indonesia, there are still few Maritime Cyber Security policies and socialization of security guarantees within government agencies. This needs to be a priority for the government, considering that technological sophistication is increasing every year and the vulnerability to cyber threats is increasing. Therefore, dealing with maritime cybersecurity is a valid and important scientific research area for marine science, especially in Indonesian waters. In this study, the MCDM method was used to obtain the right data. After that, the AHP method is used to get the priority order of the criteria. Finally, this study uses the TOPSIS method to rank the level of maritime security cyber threats with the main criteria. In addition, we performed a sensitivity analysis to observe the effect of a possible change in the criterion weights. We defined changes by six main criteria.

Among the six criteria, Human Factors (28.1%) is the most important criterion of the six evaluation components, followed by Man in the middle attack (MITM) (17%), Malware (16.2%), Outdated systems (15.4%), Phishing (15%), and Thief of credentials (8.4%). The results of the evaluation of the threat level, Economics Fraud occupies the highest threat value of 0.628 with the Cyber Sabotage level category (Level 4). There are three threats included in the Cyber Incursion level (Level 3), namely Value of cargo, Manipulation of signals used by ships, IT-systems with respective coefficients of 0.532, 0.495 and 0.445. Furthermore, six threats fall into the Cyber Theft category (Level 2), namely Firewalls (0.395), Espionage on maritime operations (0.369), State-level threat (0.351), Misuse of AIS and positioning data (0.329), Insider threat (0.279), Computer Installations (0.267). Furthermore, the results of the sensitivity analysis explain that there is no large variation in ranking order under different scenarios, and M9 becomes the most powerful cyber threat in maritime cybersecurity aspects. Thus, the proposed model is robust.

This research has real implications for qualitative analysis on aspects of cyber threats in the maritime domain in Indonesia maritime territory with increasing technological sophistication every year and increasing vulnerability to cyber threats. This research will assist stakeholders in evaluating and developing a maritime cybersecurity threat value level framework as a first step in determining a policy strategy by adopting the solutions provided in the research.

There are several limitations in this research. First, this research is devoted to evaluating the value of the threat level, however, it has not yet discussed the next step, namely the development of a maritime cybersecurity vulnerability risk analysis model in Indonesian sea territory. Future studies can discuss this risk analysis using the same method but with different criteria and alternatives in the future. Second, for further studies, a comparison of other methodologies with different multi-criteria decision-making techniques such as PROMETHEE, ELECTRE, and VIKOR can be used and the results of their application in different areas can be presented, especially in the field of financial cybersecurity and cyber defence where many criteria which can be considered. Third, this study does not discuss threat mitigation strategies as a response to reducing the risk of maritime cyber security threats. Future research may continue these studies.

Acknowledgements.

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.

Afrane, S. et al. (2022) 'Integrated AHP-TOPSIS under a Fuzzy Environment for the Selection of Waste-To-Energy Technologies in Ghana: A Performance Analysis and Socio-Enviro-Economic Feasibility Study', International Journal of Environmental Research and Public Health, 19(14). doi: 10.3390/ijerph-19148428.

Ainie, R., Saputro, G. E. and Purwantoro, S. A. (2022) 'Defense Gap Era of the Jokowi Government and Defense Economic Focus on Indonesian Maritime', Int. J. Business Management, 05(07), pp. 23–30.

Akdağ, M., Solnør, P. and Johansen, T. A. (2022) 'Collaborative collision avoidance for Maritime Autonomous Surface Ships: A review', Ocean Engineering, 250. doi: 10.1016/j.oceaneng.2022.110920.

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

Akter, S., Debnath, B. and 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), p. 100120. doi: 10.1016/j.health.2022.100120.

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

Amro, A. and Gkioulos, V. (2023) 'Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth', International Journal of Information Security, 22(1), pp. 249–288. doi: 10.1007/s10207-022-00638-y.

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.

Ashraf, I. et al. (2022) 'A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry', IEEE Transactions on Intelligent Transportation Systems, 24(2), pp. 2677–2690. doi: 10.1109/TITS.2022.3164678.

Bari, A. B. M. M. et al. (2022) 'A hybrid multi-criteria decision-making approach for analysing operational hazards in Heavy Fuel Oil-based power plants', Decision Analytics Journal, 3(May), p. 100069. doi: 10.1016/j.dajour.2022.100069.

Bodeau, D. J., Graubart, R. and 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, pp. 1147–1152. doi: 10.1109/SocialCom.2010.170.

Bolbot, V. et al. (2022) 'Developments and research directions in maritime cybersecurity: a systematic literature review and bibliometric analysis', International Journal of Critical Infrastructure Protection, 39(October), p. 100571. doi: 10.1016/j.ijcip.2022.100571.

Boutkhoum, O. et al. (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), pp. 1237–1253. doi: 10.1007/s13198-017-0592-x.

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

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.

Chang, C.-H. et al. (2021) 'Risk assessment of the operations of maritime autonomous surface ships', Reliability Engineering and System Safety, 207. doi: 10.1016/j.ress.2020.1073-24.

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

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.

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.

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

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.

Fakiha, B. S. (2020) 'Effectiveness of security incident event management (SIEM) system for cyber security situation awareness', Indian Journal of Forensic Medicine and Toxicology, 14(4), pp. 802–808. doi: 10.37506/ijfmt.v14i4.11587.

Ben Farah, M. A. et al. (2022) 'Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends', Information (Switzerland), 13(1), pp. 1–33. doi: 10.3390/info13010022.

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/24-35722737/A48026DE74D94390PQ/3?accountid=10286.

Hareide, O. S. et al. (2018) 'Enhancing Navigator Competence by Demonstrating Maritime Cyber Security', Journal of Navigation, 71(5), pp. 1025–1039. doi: 10.1017/S0373463318-000164.

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

Issa, M. et al. (2022) 'Maritime Autonomous Surface Ships: Problems and Challenges Facing the Regulatory Process', Sustainability (Switzerland), 14(23). doi: 10.3390/su142315630.

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.

Junior, W. C. L. et al. (2021) 'A triggering mechanism for cyber-attacks in naval sensors and systems', Sensors, 21(9), pp.

1–22. doi: 10.3390/s21093195.

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.

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.

Karbowski, A. (2022) 'Distributed Online Risk Assessment in the National Cyberspace', Electronics (Switzerland), 11(5). doi: 10.3390/electronics11050741.

Kuhn, K., Bicakci, S. and Shaikh, S. A. (2021) 'COVID-19 digitization in maritime: understanding cyber risks', WMU Journal of Maritime Affairs, 20(2), pp. 193–214. doi: 10.1007-/s13437-021-00235-1.

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

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

Luskatov, I. V. and Pilkevich, S. V. (2019) 'Model for Identifying Cyber Threats to Internet Information Resources', Automatic Control and Computer Sciences, 53(8), pp. 987–994. doi: 10.3103/S0146411619080170.

Lykou, G., Anagnostopoulou, A. and Gritzalis, D. (2019) 'Smart airport cybersecurity: Threat mitigation and cyber resilience controls', Sensors (Switzerland), 19(1). doi: 10.3390/s-19010019.

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.

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.

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.

Meland, P. H. et al. (2021) 'A retrospective analysis of maritime cyber security incidents', TransNav, 15(3), pp. 519–530. doi: 10.12716/1001.15.03.04.

Meland, P. H. et al. (2022) 'Assessing cyber threats for storyless systems', Journal of Information Security and Applications, 64. doi: 10.1016/j.jisa.2021.103050.

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

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.n01.0-13.

Nganga, A. et al. (2022) 'Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment', (December).

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

Octavian, A. et al. (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), pp. 195–223. doi: 10.46970/2020.26.3.3.

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. doi: 10.1016/j.ocecoaman.2023.106480.

Pradana, M. D. R. (2020) 'The Future of Shipping: Presence of Cyber Attacks in Maritime Industries', Khazanah: Jurnal Mahasiswa, 12(2), pp. 9–10. doi: 10.20885/khazanah.vol12-.iss2.art28.

Progoulakis, I., Rohmeyer, P. and Nikitakos, N. (2021) 'Cyber physical systems security for maritime assets', Journal of Marine Science and Engineering, 9(12). doi: 10.3390/jmse912-1384.

Saaty, T. L. (2008) 'Decision making with the analytic hierarchy process', International journal of services sciences, 1(1), pp. 83–98. doi: 10.1108/JMTM-03-2014-0020.

Saini, S. and 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), pp. 683–712. doi: 10.1108/JSTPM-02-2020-0032.

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.

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

Solangi, Y. A. et al. (2019) 'An integrated Delphi-AHP and fuzzy TOPSIS approach toward ranking and selection of renewable energy resources in Pakistan', Processes, 7(2), pp. 1–31. doi: 10.3390/pr7020118.

Steingartner, W. and Galinec, D. (2021) 'Cyber threats and cyber deception in hybrid warfare', Acta Polytechnica Hungarica, 18(3), pp. 25–45. doi: 10.12700/APH.18.3.2021.3.2.

Suciu, G. et al. (2019) 'Cybersecurity Threats Analysis for Airports', in New Knowledge in Information Systems and Technologies. Springer International Publishing, pp. 567–576. doi: 10.1007/978-3-030-16184-2.

Sunkpho, J., Ramjan, S. and Oottamakorn, C. (2018) 'Cybersecurity Policy in ASEAN Countries', in 17th Annual Security Conference. Las Vegas: Information Institute Conferences, pp. 1–6.

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.

Svilicic, B. et al. (2019) 'Maritime Cyber Risk Management: An Experimental Ship Assessment', Journal of Navigation, 72(5), pp. 1108–1120. doi: 10.1017/S0373463318001157.

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, Kimberly and Jones, K. (2019) 'Factors affecting cyber risk in maritime', 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2019, pp. 1–8. doi: 10.1109/CyberSA.2019.8899382.

Tam, K. and Jones, K. (2019) 'MaCRA: a model-based framework for maritime cyber-risk assessment', WMU Journal of Maritime Affairs, 18(1), pp. 129–163. doi: 10.1007/s13437-019-00162-2.

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.

Tseng, Y. P. et al. (2022) 'Selecting Key Resilience Indicators for Indigenous Community Using Fuzzy Delphi Method', Sustainability (Switzerland), 14(4), pp. 1–19. doi: 10.3390/su14042018.

Tusher, H. M. et al. (2022) 'Cyber security risk assessment in autonomous shipping', Maritime Economics and Logistics, 24(2), pp. 208–227. doi: 10.1057/s41278-022-00214-0.

You, B., Zhang, Y. and Cheng, L.-C. (2017) 'Review on Cybersecurity Risk Assessment and Evaluation and Their Approaches on Maritime Transportation', The 30th Annual Conference of International Chinese Transportation Professionals Association, (October), p. 18. Available at: https://www.researchgate.net/profile/Yunpeng_Zhang18/publication/328018682_Review_on_Cybersecurity_Risk_Assessment_and_Evaluation_and_Their_Approaches_on_Maritime_Transportation/links/5bb3d57d45851574f7f55e2e/Review-on-Cybersecurity-Risk-Assessment-and-Ev.