JOURNAL OF MARITIME RESEARCH

Vol XXI. No. III (2024) pp 209–218

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

Key Factors Of Cyber Threat In Digital Navigation Using Delphi-ISM Approach

Baruna Adi Firmanto[1,*], Adi Bandono[1], Joko Purnomo[1], Eko Krisdianto[1], April Kukuh Susilo[1]

ARTICLE INFO

Article history:
Received 17 Mar 2024;
in revised from 17 Apr 2024;
accepted 05 Jun 2024.

Keywords:
Marine Technology; Cyber threat; Digital navigation; Delphi; ISM (Interpretative Structure Modelling).

ABSTRACT

Cyber threats are illegal operations that use technology to help criminal organisations or individuals achieve their goals, whether they be political or economic. Cyber navigation in the context of maritime cybersecurity refers to the use of digital tools and systems to guarantee the efficient, safe, and effective navigation of ships. The purpose of this study is to investigate and clarify how cyber threat elements affect digital navigation. Digital Navigation Theory and Cyber Digital Theory are incorporated within its theoretical framework. A questionnaire was sent to twelve experts using the Delphi approach to determine the elements impacting cyber dangers. After this approach, eight crucial factors that contribute to cyber threats were identified. The relationships between these cyber threat elements were then mapped out using the Interpretive Structural Modelling (ISM) approach. The investigation identified four different levels of factor interaction. Internal threats (A3), firewall vulnerabilities (A4), improper use of position data, and the Automatic Identification System (AIS) are all included in Level I. Signal manipulation (A7) was recognized at Level II. Threats to IT systems (A8) and the installation of navigation equipment (A5) are included in Level III. Lastly, Level IV analyses variables that have a direct influence on cyber threats, mainly the frequency of cyber threats in Indonesia (A2) and Military Operations Other Than War (A1).

1. Introduction.

One major innovation that has become a pillar of modern human existence is the internet, which has expanded to become the world's largest and fastest platform for "borderless" social and commercial interactions that are not constrained by physical borders. Interactions are unrestricted by geographical boundaries (Wahib et al., 2022).

Ardiyanti (2014) Emphasises the rise of cyber risks, requiring new information management and security tactics. The issues resulted in the creation of the US Army Cyber Command, acknowledging cyberspace as a crucial domain on par with land, sea, air, and outer space. The US Army Cyber Command is responsible for overseeing and directing operations within the Department of Defense's information networks. Its goal is to prepare for and execute comprehensive cyber military operations to secure American interests in cyberspace and counteract various cyber threats. Cybercrime is a modern threat similar to a non-military type of warfare that can weaken national cohesion through the actions of some individuals or groups (Ariyaningsih et al., 2023).

In today's technological environment, the prevalence of various internet technologies heightens the susceptibility to foreign cyber-attacks. Integrating ships, containers, and offshore platforms into networked systems exposes businesses such as marine and energy to substantial dangers from hacker operations (Agoes, 2017).

This study examines cyber threats to digital navigation in military settings outside traditional combat. Ardiyanti (2014) Foreign naval forces have implemented strategies to address and reduce cyber threats from external sources that have the potential to disrupt or completely halt operations. Nevertheless,

[1] Indonesia Navy Technology College (STTAL), Bumi Moro, Morokrembangan, Surabaya, Indonesia 60178.

[*] Corresponding author: Baruna Adi F. E-mail Address: zackadi336@gmail.com.

cyber risks in Indonesia have not been given sufficient attention, mainly because cyber threat events are rare. This research intends to discover the aspects and interactions of cyber threats that impact digital navigation and have the potential to impair operational effectiveness. The investigation focuses on cyber hazards related to digital navigation on Indonesian Navy ships.

This study seeks to create a framework for evaluation and a simulation model for cyber security hazards that focus on digital navigation systems. This research is based on Cyber Digital Theory, Digital Navigation, and Cyber Navigation Theory in the context of maritime cybersecurity. The methodology is guided by a descriptive qualitative statistical approach, along with the Delphi method and Interpretative Structural Modelling (ISM). This method utilises knowledge from a group of twelve specialists, including scholars and professionals, throughout a research period spanning from September 2023 to February 2024. The emphasis on digital navigation as the primary research field is due to its increased vulnerability to cyber-attacks.

This project intends to create a framework for evaluation and a simulation model for cyber threats that attack digital navigation systems. This research is based on Cyber Digital Theory, Digital Navigation, and Cyber Navigation Theory in the context of maritime cybersecurity. The methodology is guided by a descriptive qualitative statistical approach, along with the Delphi method and Interpretative Structural Modelling (ISM). This method utilises knowledge from a group of twelve specialists, including academics and professionals, throughout a research period spanning from September 2023 to February 2024. The emphasis on digital navigation as the primary research field is due to its increased vulnerability to cyber-attacks.

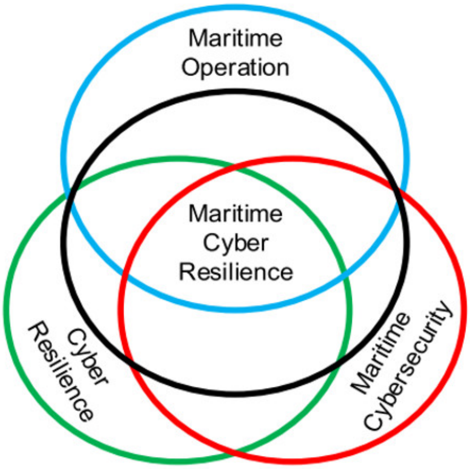
This study provides multiple contributions to the field. It broadens the existing literature on managing cybersecurity in the maritime industry (Gunes, Kayisoglu and Bolat, 2021). Secondly, it guides how marine businesses can improve their cybersecurity protocols to decrease the risk of cyber-attacks (Ejaz, Noor and Rashid, 2022). Thirdly, The research is essential for strengthening the security framework of the maritime industry by identifying weaknesses, developing solid countermeasures, and promoting best practices. Indonesia's vast maritime territory and crucial worldwide location make it susceptible to cyber-attacks, an essential topic for academic research. This study highlights a significant possibility for making both theoretical and practical contributions to maritime cybersecurity.

2. Literature Review.

2.1. Cyber Security.

Cybersecurity is a comprehensive set of practices, measures, and activities designed to safeguard systems, networks, devices, and data from cyberattacks, unauthorised access, damage, or other digital threats. These protective efforts encompass both the tangible and intangible aspects of information systems. ”soft” infrastructure of cybersecurity includes human resources, such as managers and policymakers (people), along with the policies, processes, protocols, and guidelines (processes) that collectively establish a secure environment for information systems and data. On the other hand, ”hard” infrastructure refers to the technological components, including hardware and software, essential for defending systems and data against external and internal cyber threats. Together, these elements of cybersecurity ensure the integrity, confidentiality, and availability of information systems and the data they hold (Islam, 2018).

Figure 1: The Origins of Maritime Cyber Resilience.



Source: Authors.

Putra et al. (2023) Utilise Cyber Security theory to analyse the dimensions and perform a risk assessment in the maritime cyber environment. The study uses Cyber Security theory to determine the dimensions of cyber threats and analyse the risk assessment related to cyber threats on navigation systems.

2.2. Digital Navigation.

Digital navigation, which combines satellite location, digital maps, and reference points for travel, has transformed navigation methods, but its broader effects require further investigation. Recent findings suggest notable changes in road usage, including redirecting local traffic to main roadways and a growing dependence on more minor roads. These alterations present difficulties for decision-making and the administration of maritime routes.

Digital navigation tools can predict estimated arrival times based on anticipated traffic conditions, providing a potential solution to reduce uncertainty related to trip times in busy shipping routes. The impact of digital navigation on maritime conduct is not well-documented, indicating a knowledge gap that must be addressed to improve voyage efficiency (Metz, 2022).

Asfriyanto (2012), utilized navigation theory in their study to show how the GPS system may assist air traffic control for aircraft operations in the region of Papua by acting as a remote monitoring device. This application demonstrates how navigation technology may improve both operational effectiveness and safety.

By digitalizing navigation equipment, this research seeks to overcome the vulnerabilities brought about by cyber threats, drawing on the theoretical framework previously discussed. Since cyberattacks haven't yet resulted in any damage, the perceived danger is modest, but the Indonesian Navy still needs to be ready for any possible threats. Indonesian cyber dangers are currently underestimated, which emphasizes the need for more excellent knowledge and readiness in the face of changing digital challenges.

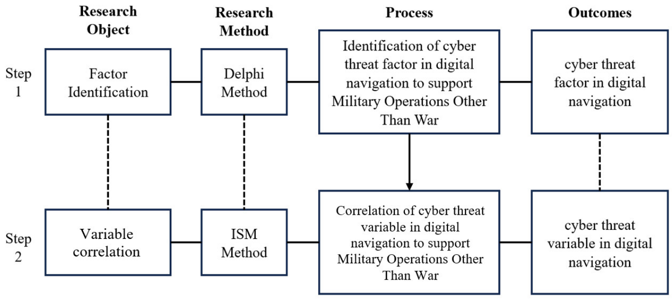
2.3. Cyber Navigation in Maritime Cybersecurity.

The worldwide maritime industry's increased reliance on digitalization, automation, and operational integration has made it more vulnerable to cyberattacks. Cyber technologies are now essential for effectively controlling and running ships and port infrastructure as well as for guaranteeing the environmental protection, safety, and security of marine operations. New risks have been brought about by the integration of operational and information technology (OT and IT) across maritime networks and their internet connectivity.

Cyberattacks are seen as a serious concern, according to the World Economic Forum's 2020 Global Risk Report, which places the maritime sector at the fifth-highest risk. Over the previous three years, there has been a 900% increase in the incidence of cyberattacks targeting OT systems in the maritime industry. According to reports, there were fifty notable cyber events in 2017, one hundred and twenty in 2018, and over three hundred the year before. Over 500 significant cybersecurity breaches will have occurred by year's end, and countless more will probably go unreported. In this regard, safety is still the top priority in maritime operations, and navigation systems are depending more and more on cyber technology to improve efficiency and security. As a result, it is more important than ever to protect maritime operations from cyber attacks. The International Maritime Organisation (IMO) has imposed strict penalties on shipowners who neglect to incorporate cyber risk management into their ship safety procedures, marking a significant step forward (Androjna et al., 2020)).

3. Methodology.

Figure 2: Research Design.

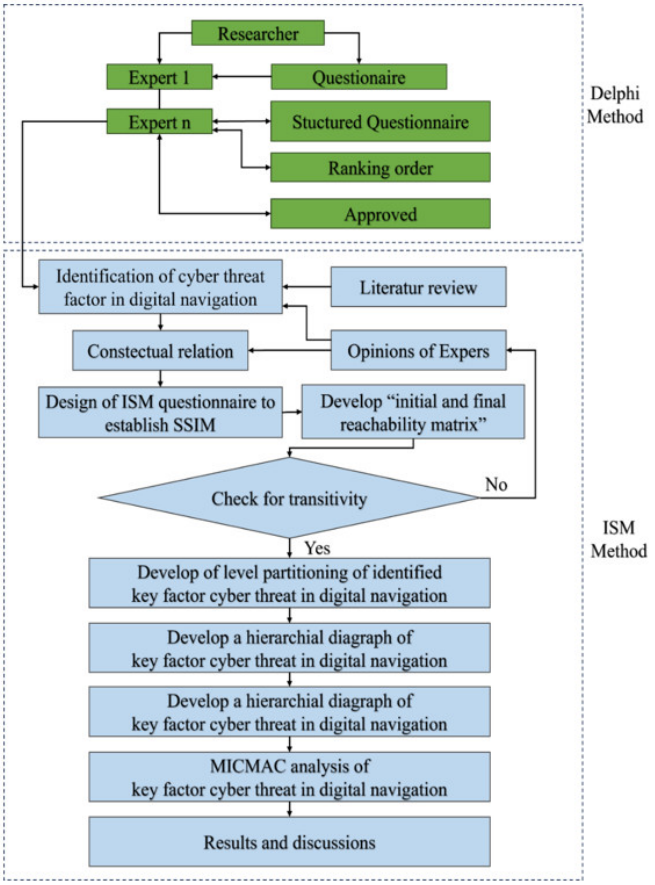

Research Object
Research Method
Process
Outcomes
Step 1
Factor Identification
Delphi Method
Identification of cyber threat factor in digital navigation to support Military Operations Other Than War
cyber threat factor in digital navigation
Step 2
Variable correlation
ISM Method
Correlation of cyber threat variable in digital navigation to support Military Operations Other Than War
cyber threat variable in digital navigation

Source: Authors.

This study used a method that developed gradually over time, starting with qualitative research and moving on to quantitative research. Primary and secondary data were the two groups into which the data collection for this study was separated. In order to gather preliminary data, experts -precisely, Ship Masters and Harbour Master officers- were surveyed and interviewed. Experts were given questionnaires to complete based on a variety of secondary data sources during the research, which was carried out inside the second fleet. As Shakeri and Khalilzadeh (2020) suggested, the optimal number of experts should be anything from six to twenty-five, based on the average consistency and correlation of their answers or viewpoints. More specialists were expected to get involved in improving the accuracy of the data utilized in the study. Twelve preselected experts in the study were interviewed, and data were gathered using questionnaires. For data analysis, the researchers used the Delphi-ISM (Interpretive Structural Modelling) method. To identify the variables influencing cyber risks in digital navigation in the context of military operations other than war (MOOTW), researchers used the Delphi technique. The elements contributing to cyber dangers in digital navigation were determined by means of questionnaires and interviews that employed the Delphi technique. The Content Validity Index was then used to assess these factors (CVI). After identifying the elements of cyber danger, researchers used the interpretative structural modeling (ISM) method to try to understand how these variables interacted with one another in the context of digital navigation.

3.1. Conceptual Framework.

Figure 3: Conceptual Framework.


Researcher
Expert 1
Questionaire
Expert n
Stuctured Questionnaire
Ranking order
Approved
Delphi Method
Identification of cyber threat factor in digital navigation
Literatur review
Constectual relation
Opinions of Expers
Design of ISM questionnaire to establish SSIM
Develop "initial and final reachability matrix"
Check for transitivity
No
Yes
Develop of level partitioning of identified key factor cyber threat in digital navigation
Develop a hierarchial diagraph of key factor cyber threat in digital navigation
Develop a hierarchial diagraph of key factor cyber threat in digital navigation
MICMAC analysis of key factor cyber threat in digital navigation
Results and discussions
ISM Method

Source: Authors.

In order to determine the variables impacting cyber threats in digital navigation for military operations other than war (MOOTW), the researcher employed the Delphi technique. The parameters influencing cyber dangers in digital navigation were ascertained with the assistance of the insights obtained from questionnaires and interviews carried out using the Delphi method. These factors were further examined via the Content Validity Index (CVI).

Having identified the variables linked to cyber dangers, the researchers set out to determine how these variables related to cyber hazards interacted with digital navigation. The method of Interpretive Structural Modelling (ISM) was employed to accomplish this.

3.2. Delphi.

With the Delphi method, a group of experts participates in a decision-making process without physically meeting and without disclosing their names to one another. This tactic aims to lessen the possibility of biased opinions and prevent any expert from taking center stage (Al-Jawhar and Rezouki, 2012). It recognizes that experts may hold different views because of their particular backgrounds, viewpoints, or analyses of the available data. As such, reaching a consensus via the Delphi technique does not always validate the validity or accuracy of the results. Instead, it represents consensus among the concerned professionals (Grossard et al., 2023).

As outlined by Pfeiffer in Karakikes and Nathanail, (2020), There are three primary phases to the Delphi technique:

a. The first questionnaire sought predictions, recommendations, and views (based on judgment or experience) from the panel of experts.

b. In the second round, each expert panelist received a summary of the first questionnaire's results so they could review their first assessment of the questionnaire using the predetermined criteria.

c. The questionnaire was returned in the third round along with details regarding the panelists' evaluation and the consensus outcomes. Once more, the panelists were invited to clarify their statements or provide justification for any disagreements with the consensus. The Delphi technique was employed in this study to determine the variables associated with cyber hazards in digital navigation. Up to three rounds of factor identification were conducted using the Delphi approach.

3.3. Content Validity Index (CVI).

For this study, the information on the research topic was gathered through written questions and in-depth interviews. Informants used Google Forms to answer these questions, making it possible to analyze their responses later. Targeting particular sources, data was gathered from mid-September 2023 until February 2024. The questionnaire items were validated using the Content Validation Index (CVI) technique in accordance with the methodology prior to distribution proposed by Shrotryia and Dhanda, (2019).

Calculations using statistical metrics like the mean and standard deviation were made to evaluate how well expert opinions converged throughout the Delphi rounds. Each research objective's importance was assessed separately by a panel of specialists using a 5-point Likert scale. The main instruments for evaluating content validity were the scale-level average content validity index (S-CVI/Ave) and the item-level content validity index (I-CVI). To be deemed acceptable, an S-CVI/Ave must be more than 0.90. Furthermore, the requirements for I-CVI differ according to the size of the panel: panels with ≤5 experts must have an I-CVI of 1.00, whereas panels with more than 5 experts must have an I-CVI of ≥0.78. When a question receives a mean score of more than 4 in expert assessments and more than 51% of experts give it a score of 4 or higher, it is considered to be in consensus and is therefore considered an essential part of the study (Alfiani and Akbar, 2020).

3.4. ISM.

The methodology known as Interpretive Structural Modelling (ISM) is an interactive learning process that aims to methodically arrange discrete but connected pieces into a comprehensive and systematic model. This approach is essential for clarifying the connections between the many parts of intricate ISM systems. By using their combined knowledge, an expert group is entrusted with using this method to ascertain the existence and type of correlations between variables (Pujotomo, Sriyanto and Widyawati, 2017). In order to create contextual linkages between variables, ISM urges researchers to include expert opinions obtained from different management strategies, such as brainstorming and the nominal group technique.

Building a Structural Self-Interaction Matrix (SSIM) is the first stage in implementing the ISM technique. In order to determine the interrelationships among elements—more particularly, how these factors influence one another—questionnaires and brainstorming sessions with respondents are used to collect the data needed to calculate the SSIM. Professionals from academia and industry are involved in identifying the contextual connections among these variables.

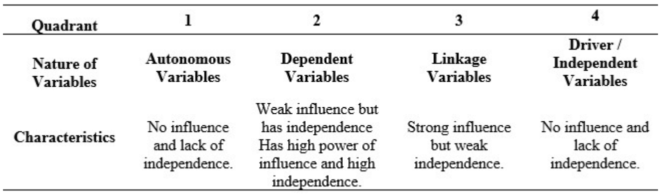
After the SSIM is constructed, it is converted into a reachability matrix. In this conversion, the reachability matrix's four SSIM symbols—V, A, X, or O—are swapped out for binary values (1 or 0). This matrix's element classification is based on the Structural Self Matrix (SSM), which makes use of the VAXO system. The VAXO system is defined as follows:

- V if $e_{ij} = 1$ and $e_{ji} = 0$.
- X if eij = 1 and eji = 1.
- A if eij = 0 and eji = 1.
- if eij = 0 and eji = 0.

A value of 1 indicates that there is a contextual relationship (or lack thereof) between the itch and the j-th items. The original reachability matrix becomes the final reachability matrix by utilizing the transitivity principle. The driving and reliance powers displayed in this final matrix are employed in the subsequent phase of the study, namely the MICMAC analysis (Shakeri and Khalilzadeh, 2020).

Next, a reachability matrix is created using the structural self-interaction matrix (SSM). The SSM's V, A, X, and O are reinterpreted as 1s and 0s, and then the transitivity rule is continually applied until a stable matrix is obtained. After meeting the transitivity requirements, this stable matrix is examined to obtain the reachability matrix, which displays the Driver Power (DP) and Dependence (D). In the final stage, the components are divided into four different sectors according to their driver power and degree of dependence: (1) Independent variables (Strong driver - Weak Dependent), which are crucial to the program's success and have a significant influence within the system; (2) Dependent variables (Weak driver - Strong Dependent), which are greatly influenced by other variables; (3) Linkage variables (Strong driver - Strong Dependent), which need to be carefully considered because they may have reciprocal effects on the system; and (4) Autonomous variables (Weak driver - Weak Dependent), which are typically isolated from the system and show minimal interrelationships (Raut, Narkhede and Gardas, 2017).

Table 1: Quadrant MICMAC.



Quadrant	1	2	3	4
Nature of Variables	Autonomous Variables	Dependent Variables	Linkage Variables	Driver / Independent Variables
Characteristics	No influence and lack of independence.	Weak influence but has independence Has high power of influence and high independence.	Strong influence but weak independence.	No influence and lack of independence.

Source: Authors.

After the preliminary study, level partitioning is the next step in the procedure. For every aspect being considered, this entails creating sets of intersections, antecedents, and reachability. Level 1 factors in the Interpretive Structural Modelling (ISM) hierarchy are those that have the same intersection and reachability sets. The method moves on to the next iteration after Level 1 elements are found and eliminated from the consideration set.

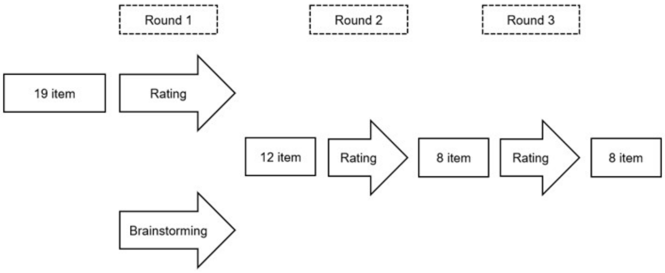
The next step involves using the reachability matrix to create a conical matrix. To complete this assignment, the elements are arranged in the order decided in the previous phase based on their hierarchical levels. In the ISM model, the factor with the highest level is positioned at the top, followed by the factor with the second level in the second position, and so on, down to the factor with the lowest level, which is positioned at the bottom (Pujotomo, Sriyanto and Widyawati, 2017).

After obtaining all required data, the following step is to create a Directed Graph (Digraph). A structural representation called a Digraph is made using the Conical Matrix and consists of nodes connected by lines that indicate the direction of the links between them. After that, the abstract nodes in this digraph are replaced with the actual factors, stated in the form of sentences, to create an ISM model. The directionality of the arrows in the model depicts the links between the elements. The ISM model uses a network of lines and nodes to represent the components and how they are related graphically. To clarify the relationships between the elements found using the Delphi and Content Validity Index (CVI) techniques, researchers utilize the ISM approach.

4. Results.

4.1. Determining the criteria using Delphi .

Figure 4: Research Procedure.



Source: Authors.

This study highlights 19 characteristics of cyber threats in digital navigation based on expert replies to questionnaires. Using the Delphi Method, the first step in generating criteria for cyber hazards was to create a round 1 questionnaire. An analysis informed this survey's design of the body of current research.

First round: A Google Form questionnaire outlining the specifics of the research objectives was given to twelve expert panels during the first phase of the project. The 19-item Likert-rated questionnaire, intended to serve as an assessment tool, took 10 to 15 minutes to complete on average. The Content Validity Index (CVI) for the items varied from a low of 0.78 to a perfect score of 1, validating all of the instrument items during this initial evaluation phase. The expert panel suggested no modifications to the themes or indicators. Seven of the sub-factors' items—Unauthorized Access (A1), Hacking (A3), Hijacking (A7), Defacing (A9), Snooping (A12), Malware (A17), and Cyber Espionage, Sabotage, and Extortion (A19)—were deleted in response to comments received during the first round of the Delphi process. As a result, the number of questionnaires was reduced from 19 to 12.

Second round: Experts were invited to evaluate the remaining 12 items' Content Validity Index (CVI) in a second round of examination. With an anticipated completion time of 10 to 15 minutes, all items were verified using a 1–5 Likert scale, as indicated by the Item CVI (I-CVI) range of 0.78 to 1. Two weeks passed between the first and second rounds. The collection of questions received an overall Scale CVI (S-CVI) of 85%, with an acceptable S-CVI of 80% or higher, and an adequate I-CVI of 81%, with a sufficient I-CVI criterion of 78% or higher. Based on the sub-criteria, four things were eliminated in this round: crackers (A18), deliberate spread of viruses (A2), sniffing (A15), spoofing (A16), and sniffing (A15). Consequently, the second round ended with the number of things being reduced from 12 to 8.

Third round: The instrument was reformulated, and after a third evaluation session that took 10 to 15 minutes to complete, it was determined to have final validity. This round produced an overall Scale Content Validity Index (S-CVI) of 87%, with the Item Content Validity Index (I-CVI) reaching 1 for nearly all items, suggesting a 100% agreement rate among the experts. The instrument's overall validity assessment is complete with this I-CVI, which is rated as very excellent. After using the Delphi technique to conduct research, eight sub-criteria were shown to be important in key factor of cyber threat.

Following the identification of the components, the Content Validity Index (CVI) was used to perform content index validation, which assessed how relevant the content requirements were to the anticipated goals.

Table 2: Results of the content validation index of the questionnaire.

No.	Threat Factors	Round 1		Round 2		Round 3		Result
		CVI	Result	CVI	Result	CVI	Result	
1	Unauthorized Access	0.75	Rejected					
2	Intentional spread of the virus	0.75	Rejected					
3	Military operations other than war	1	Accepted	0.92	Accepted	0.92	Accepted	Accepted
4	Cyber threat level	0.92	Accepted	0.83	Accepted	0.83	Accepted	Accepted
5	Hacking	0.75	Rejected					
6	Internal threats	1	Accepted	1	Accepted	0.83	Accepted	Accepted
7	Firewall	0.92	Accepted	0.83	Accepted	0.92	Accepted	Accepted
8	Hijacking	1	Accepted	0.67	Rejected			
9	Defacing	0.75	Rejected					
10	Snooping	1	Accepted	0.75	Rejected			
11	Installation of navigation equipment	1	Accepted	1	Accepted	0.92	Accepted	Accepted
12	Misuse of AIS and position data	1	Accepted	0.92	Accepted	0.92	Accepted	Accepted
13	Signal manipulation	0.92	Accepted	0.83	Accepted	0.83	Accepted	Accepted
14	IT system threats	0.92	Accepted	0.92	Accepted	0.92	Accepted	Accepted
15	Sniffing	1	Accepted	0.75	Rejected			
16	Spoofing	0.75	Rejected					
17	Malware	0.92	Accepted	0.67	Rejected			
18	Cracker	0.75	Rejected					
19	Cyber Espionage, Sabotage, and Extortion	0.67	Rejected					

*Accepted if mean >3.00; S-CVI/Ave > 0,90; if the number of experts ≤5, I-CVI = 1,00; and if the number of experts > 5, I-CVI ≥ 0,78

Source: Authors.

Twelve experts evaluated a first set of nineteen criteria in the first round of the procedure, based on the guidelines for Content Validity Index (CVI) values listed in **Table 2**. The number of validated criteria was reduced to eight after three rounds of the Delphi technique and content index validation were completed, producing pertinent and supported findings. **Table 3.** Cyber Threat Factors in Digital Navigation.

4.2. ISM Analysis.

In this part, we address cyber hazards in digital navigation using the ISM methodology. In order to build contextual links between the issues under examination, ISM methods rely on expert opinions obtained through a variety of management-related idea-generating practices (e.g., brainstorming, nominal group approaches). The ISM method's steps are as follows:

Table 3: Cyber Threat Factors in Digital Navigation.

No.	Kode	Threat Factors	Remarks
1.	A1	Military operations other than war	The act of seeking general and specific information to a target requested by the government and carried out by unauthorized individuals exploiting cyberspace.
2.	A2	Cyber threat level	The level of security from cyber threats. The higher the cyber threat level, the more vulnerable and susceptible cyber threats can be.
3.	A3	Internal threats	Attempts and activities from within are considered to jeopardize a system's integrity, security, and stability.
4.	A4	Firewall	A system or device that allows network traffic deemed secure to pass through and prevents unsecured network traffic.
5.	A5	Installation of navigation equipment	Installation of Navigation tools: during installation, hackers can easily implant viruses or systems that can be controlled from the outside.
6.	A6	Misuse of AIS and position data	AIS is a navigational tool with weak security and is vulnerable to problems and attacks such as misinformation, data corruption, and data spoofing.
7.	A7	Signal manipulation	The techniques employed by hackers to compromise or manipulate the signals received by another vessel, thereby enabling them to disrupt operations and achieve their desired outcomes.
8.	A8	IT system threats	Forms of threat to information systems include Unauthorized data transfer, Data leakage, Data deletion, Password hacking, Spoofing, and Malware.

Source: Authors.

4.2.1. Structural Self-Interaction Matrix (SSIM).

The Delphi approach was used to identify cyber threat concerns in digital navigation during the previous phase. At this point, researchers use the ISM analysis method to clarify the connections between various dangers that have been found. In order to establish a contextual relationship, the relationship between two challenges and the path that goes along with them is examined in order to analyze the variables. Then, a hypothesis regarding the contextual relationship between the challenges that have been identified is made using the idea that one challenge leads to another challenge. The experts were required to use four alphabetical codes in an 8 × 8 SSIM to complete pairwise contextual linkages between difficulties. In light of this, the relationships between challenges (i and j) have been represented by the following symbols (V, A, X, and O): V: Challenges i facilitate or influence challenges j.

A: Challenges j enable/impact on challenges i.

X: Challenges i and j are mutually interdependent (i.e., either will enable or influence the other).

O: No relationship between challenges i and j.

Table 4: Structural Self-Interaction Matrix (SSIM).

Code	Factors	A8	A7	A6	A5	A4	A3	A2	A1
A1	Military Operations Other Than War	A	A	A	A	A	X	A	
A2	Level of cyber threats	A	V	X	O	X	O		
A3	Internal threats	X	X	X	X	X			
A4	Firewall	X	A	O	X				
A5	Installation of navigation tools	X	X	X					
A6	Misuse of AIS and position data	X	X						
A7	Signal manipulation	A							
A8	IT system threats								

Source: Authors.

4.2.2. Reachability Matrix.

To create an ”Initial reachability matrix (IRM),” the symbols ”V, A, X, O” are converted into binary elements (i.e., 1, 0). The following rules are used to create the initial reachability matrix, which is displayed in Table 4:

i. If the SSIM matrix’s cell of (i, j) contains the symbol of V, the value of that cell will increase to 1 in the IRM, and the corresponding cell (j, i) will be replaced with the value ”0.”
ii. The value of cell (i, j) in the SSIM matrix will become 0, and the corresponding cell (j, i) will be replaced with the value ”1” in the IRM if the symbol of A is displayed in that cell.
iii. In the IRM, the value of cell (i, j) will become 1, and the corresponding cell (j, i) is replaced with the value ”1” if the symbol of X is displayed in the cell of (i, j) in the SSIM matrix.
iv. If the SSIM matrix’s cell of (i, j) contains the symbol O, the value of that cell will drop to 0 in the IRM, and the associated cell (j, i) will be substituted with the value ”0.”

Next, the IRM’s transitivity criteria are incorporated to create the ”Final reachability matrix (FRM).” According to the transitivity criteria, factor X inevitably impacts factor Z if it influences factor Y and factor Z is affected by factor Y.

Table 5: Final Reachability Matrix from Key Factors of Cyber Threat.

Code	Factors								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**DP***
A1	1	0	1	0	0	0	0	0	**2**
A2	1	1	0	1	0	1	1	0	**5**
A3	1	0	1	1	1	1	1	1	**7**
A4	1	1	1	1	1	1	0	1	**7**
A5	1	0	1	1	1	1	1	1	**7**
A6	1	1	1	1	1	1	1	1	**8**
A7	1	0	1	1	1	1	1	1	**7**
A8	1	1	1	1	1	1	1	1	**8**
DEP*	**8**	**4**	**7**	**7**	**6**	**7**	**6**	**6**	

*DEP = Dependence Power; DP = Driving Power

Source: Authors.

4.2.3. Level Partitions.

The hierarchy graph is formed by dividing the ultimate reachability matrix into different levels. Each problem is divided into three sets: the intersection set, antecedent set, and reachability set. The reachability set of each job consists of the task itself and any additional challenges it may provoke. It is defined as the set of entries in a particular row that includes the number 1. The antecedent set contains components with a value of 1 in a specific column, together with the challenge and any other challenges that may aid in its accomplishment. If both the reachability and intersection sets are comparable, the top-level barriers of the ISM model at level 1 are removed from the table for the next iteration set. Each assignment is awarded a level incrementally until the final challenge is determined. Table 6 provides a detailed breakdown of the level divisions for eight items over four levels.

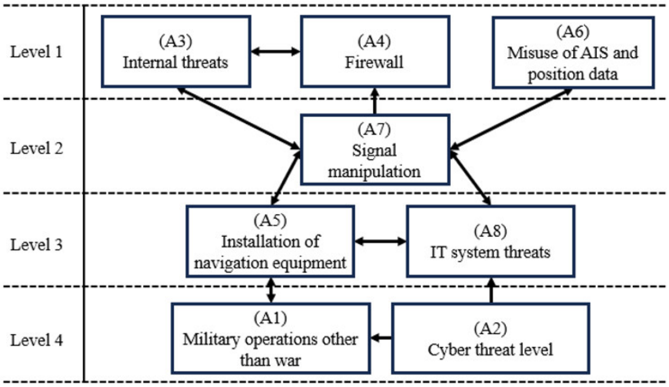
Table 6: The intersection of reachability and antecedent sets and presentation of the levels.

Code	Reachability	Antecedent	Intersection	Level
A1	1;3	1;2;3;4;5;6;7;8	1;3	4
A2	1;2;4;6;7	2;4;6;8	2;4;6	4
A3	1;3;4;5;6;7;8	1;3;4;5;6;7;8	1;3;4;5;6;7;8	1
A4	1;2;3;4;5;6;8	2;3;4;5;6;7;8	2;3;4;5;6;7;8	1
A5	1;3;4;5;6;7;8	3;4;5;6;7;8	3;4;5;6;7;8	3
A6	1;2;3;4;5;6;7;8	2;3;4;5;6;7;8	2;3;4;5;6;7;8	1
A7	1;3;4;5;6;7;8	2;3;5;6;7;8	2;3;5;6;7;8	2
A8	1;2;3;4;5;6;7;8	3;4;5;6;7;8	3;4;5;6;7;8	3

Source: Authors.

4.2.4. Building an ISM Model.

Figure 5: Hierarchical diagram of Cyber threats in digital navigation.



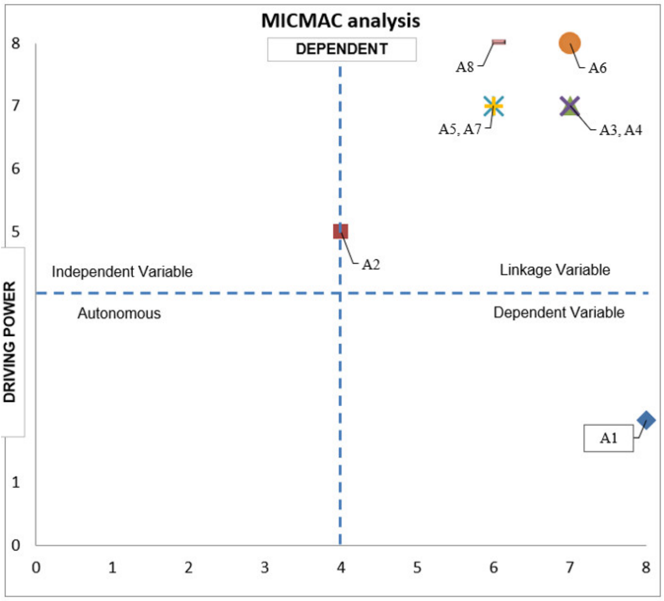
Source: Authors.

The hierarchical framework is generated as an ISM model by using the inputs from the final reachability matrix based on the partition level. An arrow from variable i to variable j, or vice versa, indicates the relationship between the two variables. Once the indirect linkages are removed, a definitive ISM model is generated. Specialists analyzed the ISM model for conceptual inaccuracies. Figure 6 illustrates the most effective digraph for implementing blockchain in a secure supply chain without any conceptual contradictions. The paradigm begins with Level I tasks at the top, followed by Level II problems in the second position, and so forth. Finally, the ISM hierarchy commences with Level VI jobs. We create the hierarchical structural model shown in Figure 5 using the division levels stated before. The elements in this diagram are organized hierarchically from level 11 to level 4.

Factors at higher levels are influenced by factors at lower levels. Factors with significant reliance power tend to have higher levels, whereas factors with strong driving powers usually have lower levels.

4.2.5. MICMAC Analysis.

Figure 6: MICMAC matrix.



Source: Authors.

A MICMAC, or ”Matrice d’Impacts Croisé Multiplication Appliquée à un Classement,” helps to understand how different blockchain adoption difficulties relate to one another in a supply chain that is cyber-secure. The driving and reliance power of the variables is examined using the MICMAC analysis, which divides the data into four groups (Etemadi, Gelder and Strozzi, 2021).

Driving variables are often represented on the y-axis, whereas dependency variables are plotted on the x-axis, as Figure 6 illustrates. The variables with weak dependence and driving capacities are shown in the first category. The fact that these variables have been grouped as ”autonomous or excluded variables” indicates that none of them are consistent with the system. Since there isn’t a single variable found in this category, there is a high degree of mutual influence between all the variables. The ”dependent variables” that make up the second category are measurements with strong dependency and weak driving. In the ISM hierarchy model, the dependent variables are located at the highest levels. ”Military Operations Other Than War” is a dependent variable in this study. The third group, referred to as ”linkage or rely variables,” is highly dependent on other factors and can drive them; any action taken on them will have a cascading effect on other variables.

The third cluster of connection includes the following in our case: ”level of cyber threats,” ”installation of navigation tools,” ”IT system threats,” ”signal manipulation,” ”internal threats,” ”firewalls,” and ”misuse of AIS and position data.” Addressing one of these issues will have an impact on the others. ”Driving factors” are associated with good driving abilities and weak reliance.

5. Discussion.

An integrated method was used to create the study’s final model of cyber danger elements in digital navigation (in three rounds of Delphi and ISM). Experts agree on two prominent selection indices, which served as the foundation for this model’s construction. In order to determine the parameters for analyzing data from expert-approved Delphi methodologies and qualitative interviews, this study used open and axial coding analysis. A total of eighteen criteria were selected to warrant additional study. The expert panel looked over the results of the MICMAC approach as well as the interpretive structural model in order to minimize inaccuracies. The specialists were happy that it could take into account potential elements connected to the current situation. A structural discussion based on the factorization levels found in the ISM model is used to present the results.

In order to identify and model cyber danger aspects in digital navigation, the ISM technique is applied. There are four stages in the model. Figure 5 shows that level 1 dangers include internal threats (A3), firewalls (A4), and misuse of position data and AIS (A6). As linkage variables, these three elements in the MICMAC analysis exhibit a high degree of reliance and driving forces. An internal threat poses a risk to an organization since some plot to undermine established plans. In the upcoming years, companies plan to increase their expenditure against insider attacks (Gheyas and Abdallah, 2016). Systems or devices known as firewalls permit network traffic that is considered secure to get through while blocking unsecured network traffic (I. Nengah Putra et al., 2023). Therefore, analyzing firewall platforms and how they affect network performance is crucial to determining how successful network security is. AIS is now a standard piece of navigational equipment on all ships. Nevertheless, the security of this equipment is lacking, making it susceptible to issues and assaults, including disinformation, data corruption, and data spoofing (Zhang et al., 2006).

Figure 5 illustrates the lowest levels of cyber threat (A2) and military operations other than war (A1). On the other hand, the MICMAC displays variables with a small driving force but significant dependence on different factors. In military operations other than war, unauthorized personnel use cyberspace to obtain general and detailed information about a target at the government’s request (Nindy et al., 2002). The degree of protection against cyber threats is known as the cyber threat level. Cyber dangers might be more prone to vulnerability, and the level of cyber threats might be higher (I. Nengah Putra et al., 2023).

The MICMAC analysis displays three significant types of variables, along with their relative importance, based on the interdependencies and motivating factors of each variable. The first cluster to be autonomous is the autonomous cluster. These variables have little effect on the system as a whole because of their low reliance and driving force. There aren’t any autonomous variables in this study. This study so demonstrates the significance of all the variables.

Dependence cluster: variables with a substantial dependence but a weak driving force. The cyber threat level (A2) and military actions other than war (A1) are dependent elements in this study.

Linkage Cluster: a cluster of variables with high ”strength of dependence” and ”strong driving force” that is considered ”linkage” in nature. This means that any action taken on one variable will have an impact on other variables and have a feedback effect on the original variables. The factor is unstable as a result. Internal threats (A3), firewalls (A4), misuse installation of navigation tools (A5), AIS and location data (A6), signal manipulation (A7), and IT system threats (A8) are the six factors in Linkage clusters that are examined in this study.

High driving power and low dependency variables are critical to the independence cluster and are categorized as crisis factors. There aren't any independent factors in this study. This study so demonstrates the significance of all the variables.

5.1. Implications.

This section includes two parts: theoretical implications of cyber risks for digital navigation and consequences for managerial practice.

Theoretical. This study can address the academic and scientific gap by offering a thorough understanding of the driving forces behind cyber dangers in digital navigation. This study demonstrates that Military Operations other than war and cyber threat levels are now the primary factors influencing cyber risks in digital navigation. Cyber dangers impact digital navigation and operational success.

A hierarchical model of the identified factors was created utilizing the ISM technique. This model illustrates the hierarchy and connections among the components discovered in cyber risks. The ISM technique categorizes these components in a hierarchy and identifies 8 categories. The connections among the 8 elements are also explained. The results demonstrate that all parameters are interconnected, suggesting their significance. We use ISM to gain fresh insights into the relationships between factors. We present this as a crucial inference for understanding cyber. Another important implication is understanding linkages between variables and how these interactions are manifested in their dependencies and driving forces, as well as in relation to other variables. This research does not delve into the detailed correlations among various driving elements and their interactions. Subsequent studies could investigate the correlations among certain influencing elements.

Managerial/Practical Implication. This study can assist practitioners and decision-makers in comprehending and identifying novel techniques that can be implemented. This research offers a well-structured conceptual model to investigate cyber risks among policy stakeholders in defense capabilities development, contributing fresh perspectives to the existing literature. This framework provides a thorough comprehension of cyber threat elements that can impact the effectiveness of operations.

Secondly, this model will assist the government in identifying potential dangers that could impact the transportation of commercial vessels. The government can devise a strategy to address the issue and offer cyber training to commercial ship crews. These will aid politicians and educational institutions in exploring alternative avenues beyond the military using a systematic approach. This research will enhance understanding of cyber issues, particularly in the Indonesian maritime domain.

Conclusions.

Research on cyber risks to digital navigation is a delicate field because of navigation's crucial role in operational security and its typically secret nature. The rapid technological improvements, especially in the cyber sector, need a review of the suitability of present defense systems to address the range of cyber threats. Studying potential cyber dangers in maritime navigation and other military platforms like tanks and fighter jets is an essential and legitimate subject of scientific research for the military, marine, and maritime sciences. This study utilizes the Delphi approach to collect expert opinions on factors influencing cyber risks. Then, it applies the Interpretive Structural Modeling (ISM) method to analyze the correlations among these elements. The research emphasizes that Military Operations Other Than War (MOOTW) and the current level of cyber threats in Indonesia are crucial factors that can increase the risk of cyber threats to the navigation systems of Indonesian Navy Vessels. Level III factors include the installation of navigation equipment on vessels (A5) and risks to IT systems (A8). Level II identifies signal manipulation in vessels (A7) as a potential concern. Level I encompasses internal threats (A3), firewall vulnerabilities (A4), and the misuse of AIS and position data, which are controlled but significant in the cyber threat landscape.

This study provides insights on how to analyze cyber threats in the Indonesian Navy's defense equipment sector, considering the growing technological complexity and variety of new threats. It intends to assist stakeholders in assessing and constructing a framework for marine cyber threats that could affect operational success. It also functions as an initial stage in developing policy initiatives by implementing suggested solutions.

Limitations and future research.

Nevertheless, the research is subject to various constraints. Initially, it assesses cyber threats to digital navigation in Indonesian maritime areas without creating a risk analysis model for these threats. Future studies could further investigate this by using the same methods to examine various criteria and options for risk assessment.

Secondly, our analysis is exploratory because we utilized the Delphi approach. Future research could use questionnaire-based surveys and gather data from more stakeholders to investigate potential cyber-related hazards.

This research does not explore techniques to mitigate dangers and minimize the impact of cyber threats, nor does it evaluate the seriousness of cyber threats to prioritize them. These regions present a rich ground for additional research, which could lead to a more thorough comprehension and control of cyber dangers in the maritime sector.

Acknowledgements.

Gratitude is expressed to Sekolah Tinggi Teknologi Angkatan Laut (STTAL) for the contribution to the completion of this research and to the interviewees for participating in this research.

References.

Al-Jawhar, H.D. and Rezouki, S.E. (2012) 'Identification of Procurement System Selection Criteria in the Construction Industry in Iraq by Using Delphi Method', International Proceedings of Economics and Development Research 2012, pp. 142–147.

Alfiani, T. and Akbar, N. (2020) 'Exploring Strategies to Enhance Zakat Role to Support Sustainable Development Goals (SDGs)', International Conference of Zakat, (1989), pp. 295–310. Available at: https://doi.org/10.37706/ iconz.2020.226.

Androjna, A. et al. (2020) 'Assessing cyber challenges of maritime navigation', Journal of Marine Science and Engineering, 8(10), pp. 1–21. Available at: https://doi.org/10.3390/jmse-8100776.

Ardiyanti, H. (2014) 'Cyber-Security Dan Tantangan Pengembangannya Di Indonesia', pp. 95–110.Ariyaningsih, S. et al. (2023) 'Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia', Justisia: Jurnal Ilmu Hukum, 1(1), pp. 1–11.

Asfriyanto, T. (2012) 'Designing and Building a Navigation System As a Long Distance Monitoring Using Gps Which Operate in Papua Province in Tiom-Wamena Route', Indept, 2(3).

Ejaz, S., Noor, U. and Rashid, Z. (2022) 'Visualizing Interesting Patterns in Cyber Threat Intelligence Using Machine Learning Techniques', Cybernetics and Information Technologies, 22(2), pp. 96–113. Available at: https://doi.org/10.2478/ cait-2022-0019.

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

Etemadi, N., Gelder, P. Van and Strozzi, F. (2021) 'An ISM Modeling of Barriers for Blockchain / Distributed Ledger Technology Adoption in Supply Chains towards Cybersecurity Infrastructure safety View project Predicting floodplain velocities due to embankment dam failure of Mosul dam View project An ISM Mod', Susta, 13(9), p. 4672. Available at: https://doi.org/-10.3390/su13094672.

Gheyas, I.A. and Abdallah, A.E. (2016) 'Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis', Big Data Analytics, 1(1). Available at: https://doi.org/10.1186/s41044-016-0006-0.

Grossard, C. et al. (2023) 'Building the design ICT inventory (DICTI): A Delphi study', Computers in Human Behavior Reports, 9(January), p. 100261. Available at: https://doi.org/-10.1016/j.chbr.2022. 100261.

Gunes, B., Kayisoglu, G. and Bolat, P. (2021) 'Cyber security risk assessment for seaports: A case study of a container port', Computers and Security, 103, p. 102196. Available at: https://doi.org/ 10.1016/j.cose.2021.102196.

Islam, M.J. (2018) 'Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index', Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi dan Komunikasi, 8(2), p. 137. Available at: https://doi.org/10.17933/mti-.v8i2.108.

Karakikes, I. and Nathanail, E. (2020) 'Using the delphi method to evaluate the appropriateness of urban freight transport solutions', Smart Cities, 3(4), pp. 1428–1447. Available at: https://doi.org/10.3390/smartcities3040068.

Metz, D. (2022) 'The impact of digital navigation on travel behaviour', UCL Open Environment, 4, pp. 1–10. Available at: https://doi.org/10.14324/ 111.444/ucloe.000034.

Nindy, B. et al. (2002) 'Peran dan Strategi TNI AL dalam Pengamanan Alur Laut Kepulauan Indonesia II (ALKI II) Melalui Operasi Militer Selain Perang (OMSP)', (Alki Ii), pp. 1–25.

Pujotomo, D., Sriyanto, S. and Widyawati, L. (2017) 'Analisis Penghalang Implementasi Cleaner Production Di Kampung Batik Semarang Dengan Pendekatan Interpretive Structural Modeling', None, 6(1).

Putra, I N. et al. (2023) 'A hybrid AHP-TOPSIS for risk analysis in maritime cybersecurity based on 3D models', Decision Science Letters, 12, pp. 759–772. Available at: https://doi-.org/10.5267/dsl.2023.6.005.

Putra, I. Nengah et al. (2023) 'Cyber Threat Analysis of Maritime Cybersecurity Using AHP-Topsis', Journal of Maritime Research, 20(2), pp. 13–24.

R. Agoes, E. (2017) "'Cybercime" Dan Kaitannya Dengan Beberapa Kegiatan Di Laut', Jurnal Bina Mulia Hukum, 1(2), pp. 99–110. Available at: https://doi.org/10.23920/jbmh.v1n2-.11.

Raut, R.D., Narkhede, B. and Gardas, B.B. (2017) 'To identify the critical success factors of sustainable supply chain management practices in the context of oil and gas industries: ISM approach', Renewable and Sustainable Energy Reviews, 68(June 2016), pp. 33–47. Available at: https://doi.org/10.1016/j.rser.20-16.09.067.

Shakeri, H. and Khalilzadeh, M. (2020) 'Analysis of factors affecting project communications with a hybrid DEMATEL-ISM approach (A case study in Iran)', Heliyon, 6(8), p. e04430. Available at: https://doi.org/10.1016/j.heliyon.2020.e04430.

Shrotryia, V.K. and Dhanda, U. (2019) 'Content Validity of Assessment Instrument for Employee Engagement', SAGE Open, 9(1). Available at: https://doi.org/10.1177/21582440188-21751.

Wahib, P. et al. (2022) 'Sosialisasi Cyber Security Untuk Meningkatkan Literasi Digital', Abdi Jurnal Publikasi, 1(2), pp. 64–68. Available at: https://jurnal.portalpublikasi.id/index.php-/AJP/article/view/21%0Ahttps://jurnal.portalpublikasi.id/index-.php/AJP/article/download/21/14.

Zhang, X.G. et al. (2006) 'Research on sea digital map used for ship navigation', International Geoscience and Remote Sensing Symposium (IGARSS), 4, pp. 872–875. Available at: https://doi.org/10.1109/IGARSS.2006.224.