ECDIS Cyber Security Dynamics Analysis based on the Fuzzy-FUCOM Method

Gizem Kayişoğlu[1], Bünyamin Güneş[2], Pelin Bolat[1]

ECDIS is one of the most important pieces of navigational and information equipment on board ships, as well as a vital component of the ship's cyberspace. ECDIS has cyber vulnerabilities because of its connections to external systems like RADAR or GPS, sensors via serial (IEC61162-1/2), analogue, and digital interfaces, as well as onboard Wi-Fi, internet, and LAN technologies. This study identifies and ranks the cyber risks that cause ECDIS control loss, as well as the barriers that can be put in place to stop them, the potential consequences if they are not stopped, and the mitigations that can be utilised to avoid them. Due to a lack of historical data and research on identifying and prioritising ECDIS cyber security dynamics in the literature and the fact that this field necessitates specialised knowledge in terms of computer science and operational maritime navigation, the Fuzzy Triangular Full Consistency Method (FUCOM-F), based on expert opinion, is used in this study. Then, a bow-tie framework is employed to visualize the dynamics of ECDIS cyber security and their hierarchical classification from the analysis as a cyber-architecture. The results indicate that the primary cyber threat for ECDIS is "malware infection via the internet and intranet (M1)." The primary potential consequence, in the event that these cyber threats targeting ECDIS cannot be prevented, is the unavailability of the system (O1). The most efficient barriers against M1 attacks are “up-to-date virus protection” and “scanning software," while the most crucial measure to prevent the impact of O1 is "network segregation." Consequently, in addition to its strong methodological foundation, this research offers significant benefits to maritime professionals and cybersecurity experts by providing valuable insights on preventing cyber-attacks on bridge system infrastructure, particularly ECDIS.

KEY WORDS

~ ECDIS cyber security
~ Maritime cyber security
~ FUCOM
~ ECDIS IT and OT dynamic

[1]Istanbul Technical University, Maritime Faculty, Istanbul, Türkiye
[2]Ministry of Transport and Infrastructure, Maritime General Directorate, Ankara, Türkiye

e-mail: yukselg@itu.edu.tr

doi: 10.7225/toms.v13.n01.w09
Received: 28 Aug 2023 / Revised: 23 Dec 2023 / Accepted: 26 Jan 2024 / Published: 20 Feb 2024

1. INTRODUCTION

Cybersecurity in the maritime field is about the physical and information infrastructures where cyberspaces intersect with maritime areas. Ships appear as critical infrastructures or structures with information, communication, and navigation technologies integrated with industrial control systems. As technology continues to evolve, information technology (IT) and operational technology (OT) onboard ships are increasingly being connected to each other and to the world-wide network. This integrated network poses a great risk in terms of malicious attacks and unauthorised access to the ship's systems and networks (BIMCO, 2020). From this perspective, all machinery, navigation, and communication systems on a ship can be exposed to cyber threats. These threats can be performed by technical human error in the system or software or by cybercriminals by finding weak points or vulnerabilities in the system (Steven, 2016). In this regard, cyber security is not only a concept of information risks any more, where many potential risks have emerged to the safe operation of ships, but it also requires understanding and analysing those risks.

In light of the ship environment, the Global Positioning System (GPS), Automatic Identification System (AIS), and Electronic Chart Display and Information System (ECDIS) are the primary electromagnetic field-based communication and networking technologies used on bridges (Ben Farah et al., 2022). Ships also have the Radio Detection and Ranging Device (RADAR), the Voyage Data Recorder (VDR), the International Maritime Satellite (INMARSAT), communication systems like Very High Frequency (VHF) and Voice Over Internet Protocol (VOIP), and integrated bridge systems that get feedback from a lot of sensors and a compass. However, ECDIS is the main subject of this study.

ECDIS is one of the significant information and navigation equipment onboard vessels. Convention on the Safety of Life at Sea (SOLAS) regulation V/19 requires international vessels to carry ECDIS with some criteria from 2011. As Svilicic et al. (2019a) also stated, ECDIS must be type-approved, including updated ENCs, software maintenance, and backup arrangements to meet on-board fulfilment criteria of ECDIS (IMO, 2017; IMO, 2006; IHO, 2017). According to their function and configuration system (FURUNO 2018), it involves computer technology and marine electronics that meet IT and OT standards. The primary specifications take place in the International Electrotechnical Commission (IEC) standards, such as IEC 61162-1/2/450 (2016; 1998; 2018), IEC 62065 (2014), IEC 61174 (2015), and IEC 62288 (2021). These interfaces, which transmit serial, digital, and analogue data from external sources to ECDIS, include vulnerabilities that allow unwanted network access, denial of service (DoS), system corruption, unavailability, and tampering. IEC 61162-1 and -2 are protocols harmonised with National Marine Electronics Association (NMEA) protocols, like NMEA 0183 and high-speed NMEA 0183 interfaces for identifying, data transmission protocol, electrical signal requirements, time, and specific sentence formats for a 4800-baud serial data bus for marine electronic devices. Tran et al. (2021) noted that NMEA 0183 lacks encryption, authentication, and validation. Thereby ship speed, location, depth, and other NMEA 0183-compatible data are provided to ECDIS in sentences with printable ASCII characters. Without these security measures, NMEA 0183 devices like ECDIS are vulnerable to cyberattacks, including spoofing-packet sniffing, and man in the middle attacks (Svilicic et al., 2019b). NCC Group, a security outfit, has shown that ECDIS can be influenced and infiltrated (Alekseenkov et al., 2021). They uncovered download, reading, deletion, relocation vulnerabilities and cyberattack methods. Viruses can be introduced via a removable USB disk: one of the various systems hooked into ECDIS by a crew member, ship, or visitor exploiting an unpatched vulnerability over the internet. According to Kessler et al. (2019), attackers implant malware into ships' ECDIS via satellite. The malware changes the ship's position during the night without updating the ECDIS. Due to its connections to external systems, sensors, onboard Wi-Fi or internet, Local Area Network (LAN), and VOIP technologies, the ECDIS is vulnerable to worms, viruses, ransomware, and Trojans. Due to vulnerabilities targeted cyber-attacks, ECDIS is a vital ship cyber space. Cyberattacks on ships can cause navigation accidents,

economic losses, environmental damage, and death. Analysing cyber security dynamics can help shipping companies mitigate cyberattacks and improve ship cyber resilience.

From this point of view, this study aims at prioritising cyber security controls for ECDIS by considering cyber threats and their potential consequences. For this purpose, firstly, (i) ECDIS cyber threats, (ii) the barriers allowing to prevent these threats, (iii) the potential consequences of these threats, and (iv) the mitigations allowing to prevent these consequences are identified as ECDIS cyber security dynamics. Furthermore, Fuzzy Triangular Full Consistency Method (FUCOM-F) is used to weight the importance level of the ECDIS cyber security dynamics. Finally, the findings derived from FUCOM-F analysis are presented in a bow-tie framework in terms of demonstrating a hierarchical order so as to show ECDIS cyber risks and their mitigations process as a holistic and demonstration approach. Beside its robust methodological background, this research provides utmost contributions towards maritime professionals and cybersecurity experts, with helpful insights into cyber threats prevention to bridge system infrastructure, specifically ECDIS.

The structure of the study is outlined as follows: In the introduction section, the research problem is given as identifying ECDIS cyber security dynamics and weighing their importance via the fuzzy FUCOM method. In the literature review section, by introducing studies related to maritime cyber security risk assessment, ECDIS cyber security, and the FUCOM methodology, it is stated that the prioritisation of the ECDIS cyber security dynamics via the FUCOM-F method is a new implementation in the literature. In the methodology section, after presenting the implementation steps of the FUCOM-F method, the analysis is conducted for ECDIS cyber security dynamics. In the findings sub-section, the results of the FUCOM-F analysis are presented for ECDIS cyber security dynamics. In the next sub-section, the dynamics are hierarchically positioned on the bow-tie diagram, according to the ranking of the dynamics based on the findings of the FUCOM-F analysis. In this way, the entire result of the FUCOM-F can be demonstrated as a holistic view. In the discussion section, strategies as a guide for ship officers who are responsible for ECDIS cyber security, company managers, and even insurers in any cyber incident to make policy on the proposed hierarchical diagram are given for all ECDIS cyber security dynamics. In the conclusion section, the contributions and limitations of the study are introduced.

2. LITERATURE REVIEW

Academic studies, cyber events, and reports in the maritime sector have revealed that ECDIS contains several cyber vulnerabilities that cause critical consequences for ships, such as collision and grounding of the ship, and suggested that a risk assessment should be made for ECDIS (Svilicic et al., 2019b; 2019c; Tam & Jones, 2019; Androjna et al., 2020). Accordingly, there are a limited number of studies focusing directly on ECDIS cyber security in the literature (Hareide et al., 2018; Park et al., 2021; Svilicic et al., 2019a; 2019d; 2019e; Kayisoglu et al., 2022). In most of them, risk assessment approaches for maritime cyber security are offered, and the frameworks offered are performed on ECDIS as a case study. For instance, Svilicic et al. (2019a; 2019d) detected vulnerable servers and operating systems of ECDIS via a penetration test tool and stated some cyber-attacks against these parts of ECDIS, such as unauthorised access and denial of service attacks. In another study, they offered general mitigation for ECDIS cyber vulnerabilities, such as crew training, up-to-date operating systems, and cyber security policies (Svilicic et al., 2019e). Hareide et al. (2018) highlighted cyber security awareness for integrated bridge systems and presented some possible ECDIS cyber-attacks. Park et al. (2021) presented ECDIS vulnerability improvement factors and prioritised them according to the skill of navigation officers. Finally, DNV-GL has issued a recommended practice for stakeholders to understand and analyse cyber risks for ships (DNV-GL, 2016). The practice was initially based on the mapping of the OT and IT of the ships. Additionally, it offers a comprehensive approach including assessment, improvement, and validation on managing cyber security risks for both ships and mobile offshore units in the maritime shipping industry.

However, to the best of the author's knowledge, the detailed identification of ECDIS cyber vulnerabilities, cyber threats, and detection and mitigation of them, as well as the whole consideration of them in the ECDIS cyber security system and the weighting of each asset of ECDIS cyber security, have not been encountered in the literature. Although a number of risk assessment studies of ECDIS cyber security exist in the literature, it is evident that the limited cyberattacks against ECDIS have not yet been addressed. Therefore, limited suggestions on mitigations for ECDIS cyber security have been offered. In addition, they have not taken into consideration which barriers and mitigations are more important in themselves to ensuring ECDIS cyber security. They have not presented a hierarchical cyber security system for ECDIS in terms of threats, barriers, consequences, or mitigations.

On the other hand, by reviewing the literature in terms of specific cyber risk assessment methodologies in the maritime sector, it may be seen that different approaches are used for this purpose. Kala and Balakrishnan (2019) have identified cyber risks within maritime shipping and focused on cyber preparedness in a global maritime context. Accordingly, they have proposed some concepts, such as people, processes, technology, and operations factors, to be used in any kind of shipping cyber risk management in their study. Kavallieratos and Katsikas (2020) have offered "STREAD" and "DREAD" methodologies for the identification and analysis of emerging threats on ships, both qualitatively and quantitatively. Bolbot et al. (2020) have proposed the Cyber-Preliminary Hazard Analysis method, which is integrated and enriched with new steps supporting the identification of cyber-attack scenarios and risk assessment implementation on an inland waterway autonomous vessel's navigation and propulsion systems. Tam and Jones (2019) have proposed a model-based framework for maritime cyber-risk assessment, named MaCRA. Their proposed framework consists of the characterisation of maritime cyber-risks and their severity, scalable measurements from single systems or ships to fleets, identification of both systems and top risks, as well as providing risk data to support human decision-making. Furumoto et al. (2020) have evaluated possible cyber-attacks on near-future ships as smart ships. In their study, the architecture and topology of the ships were analysed according to possible attack scenarios, which will be helpful in establishing cyber security risk management for the intended ship. However, just to state the context of the studies mentioned above, the proposed cyber risk assessment approaches have been more specifically proposed for general maritime cybersecurity, and most of them have not specifically covered ECDIS cybersecurity. In addition, those related to ship cyber security risk studies seem to focus more on navigation safety. Moreover, the proposed methodologies present the cyber risk level of the considered system, but they have not prioritised the suggested mitigations for risky threats and their consequences.

There have recently been many techniques and tools for maritime cyber security risk assessment in the literature. Hemminghaus et al. (2021) have introduced a comprehensive BRidge Attack Tool (BRAT), interactively presenting numerous attack implementations aimed against nautical data transfer in maritime systems. Park et al. (2023) have proposed a framework that integrates Failure Mode and Effects Analysis (FMEA) with a rule-based Bayesian Network (RBN) for evaluating the risk levels of identified threats and gaining a deeper understanding of the threats that have the greatest impact on the overall cybersecurity risk in the maritime sector. Similarly, Soner et al. (2023) have implemented the FMEA technique for VDR cyber security risk assessment. Amro and Gkioulos (2023) have presented a cyber risk assessment approach to cyber physical systems, including maritime, energy, and manufacturing that is FMECA-ATT&CK, which means Failure Mode, Effects, and Criticality Analysis (FMECA), with respect to the Adversarial Tactics, Techniques, and Common Knowledge framework (ATT&CK). Progoulakis et al. (2023) have claimed that the API Security Risk Assessment (SRA), Bow Tie Analysis (BTA), Cyber-PHA (Process Hazard Analysis), and MITRE ATT&CK Threat Model are some of the assessment methods for cyber and physical security. They have found that the application of BTA for a security breach incident targeting a port access security system is showcased to demonstrate both proactive and reactive measures taken to mitigate such attacks. Melnyk et al. (2023)

have suggested methods for detecting cyber threats and provided a probabilistic evaluation of ship cybersecurity. The evaluation is based on a comprehensive approach to measuring the susceptibility of essential equipment and systems on board the ship. Harish et al. (2024) have presented a tool called BridgeInsight, representing an asset profiler for penetration testing in a heterogeneous maritime bridge environment. Erstad et al. (2023) have introduced a Cyber Emergency Response Procedure (CERP) that offers a structured approach for organisations to enhance their crews' ability to respond to a cyber crisis, taking into account their operational context.

There is a critically low number of studies aiming at the prioritisation of cyber dynamics for the maritime sector in the literature. One of those studies was presented by Karahalios (2020). Karahalios (2020) has proposed a risk-based methodology for ship cyber threats via STPA-SafeSec's analysis and the Fuzzy Analytic Hierarchical Process (FAHP). The cyberattacks against ships in a case of piracy have only been ranked with the FAHP method. Another study that is closest to this purpose has been presented by Yoo and Park (2021). In the study, they have made a qualitative risk assessment of cybersecurity, which contains vulnerability enhancement plans for digitalised ships. Based on the risk assessment, they have conducted a survey in the study, and the results have been analysed via the AHP method for the development of improvement of planned priority measures. Finally, Shang et al. (2019) have used an AHP method including an attack tree model, combined with triangular fuzzy numbers, in order to evaluate industrial control system cyber risks. Accordingly, it may be seen that the prioritisation of cyber dynamics for ECDIS within a whole system has not been considered in the literature yet.

To the best of the author's knowledge, the utilisation of fuzzy FUCOM for maritime cyber security has not yet been investigated. Despite the fact that FUCOM is a new model, there is specific research that utilises the advantages of FUCOM in different fields. Pamucar et al. (2020) have used the FUCOM to prioritise transportation demand management measures by addressing the case study in Istanbul's urban mobility system. Pamucar et al. (2018) have demonstrated the use of the FUCOM-MAIRCA multi-criteria model to assess level crossings, while installing security equipment. Badi and Abdulshahed (2019) have demonstrated the utilisation of the FUCOM in assessing air traffic lines. Noureddine and Ristic (2019) have employed a hybrid FUCOM-MABAC model to assess the routes for transporting hazardous materials via road traffic. Furthermore, the FUCOM has been utilised in the logistics domain for tasks, such as choosing equipment for storage systems (Fazlollahtabar et al., 2019), sustainable supplier selection (Matić et al., 2019), and managing supply chains (Erceg & Mularifović, 2019). Lastly, there are some studies that have implemented FUCOM with fuzzy techniques on cyber security for different systems, such as cyber risk evaluation of general security technologies (Erdogan et al., 2020) and cyber risk evaluation in energy management and control systems (Alhakami, 2023). As can be understood from this, FUCOM-F is an appropriate and preferable technique for cyber security in any field.

In contrast to the aforementioned research, this study takes a comprehensive approach to addressing the ECDIS cyber security system. The prioritisation values for ECDIS cyber security dynamics are derived using a distinct method (FUCOM-F), which differs from the methods employed for other cyber security topics in the literature. Therefore the application of a novel weighting method is introduced to the literature, specifically focusing on the cyberspace of ships (ECDIS) in the context of maritime cybersecurity. Ultimately, the entire system presentation is showcased using a bow-tie framework. This study offers a thorough and meticulous assessment of ECDIS cyber security, thereby providing a significant contribution to both academic and industry sectors.

3. METHODOLOGY

This study aims at examining the cyber security system for ECDIS onboard ships. For this purpose, firstly, the cyber threats exploiting ECDIS vulnerabilities and the consequences that may occur as a result of the realisation of these threats are revealed by the solution proposals recommended in the DNV-GL report to ensure cyber security in the maritime sector (DNV-GL, 2016). Besides, the technological standards and qualifications of ECDIS, as well as the weaknesses of this infrastructure have been revealed and analysed by researching the literature, including the operational handbook of ECDIS, its standard type approval certificate, catalogues of ECDIS manufacturers receiving type approval, and ITU standards (IHO, 2012; 2017; 2019; IMO, 2006; Weintrit, 2009). Subsequently the barriers are defined to prevent these threats towards ECDIS by referencing the recommendation of the DNV-GL report (2016), which is on maritime cyber security. If these threats occur despite the developed barriers, then the consequences towards ECDIS are identified from literature and technical reports. Lastly, the mitigations are determined to prevent critical consequences for ECDIS.

After that, FUCOM-F is used to understand the importance weighs of the identified threats, barriers, consequences, and mitigations for ECDIS cyber security. The results of the analysis provide the prioritisation values of these factors in the system for ECDIS cyber security. According to the prioritisation values, the bow-tie diagram is created to show the overall dynamics for ECDIS cyber security in one single hierarchical diagram.

Essentially, the bow-tie model is developed to provide reactive and proactive risk management in an accident scenario by showing the reason for the unwanted event on the left side and the possible effects of it on the right side if the event has happened. The advantages of the bow-tie method are simple reading and understanding of threats, barriers, and consequences in a system. It is also aimed at clearly showing the initiating cases, keyhole barriers and escalators, possible outcomes, recovery measures, and the way of their combination. Finally, it presents a safety management system via the linkage of the barriers (Mokhtari et al. 2011). The function of the bow tie can be seen in Figure 1 (Merrett, 2019). In this study, a bow-tie diagram is used because of these advantages. The prioritisation values obtained from FUCOM-F are used to understand where identified factors take place in the bow-tie diagram. Consequently, the bow-tie model provides an effective single diagram to demonstrate the ECDIS cyber security system in this study.

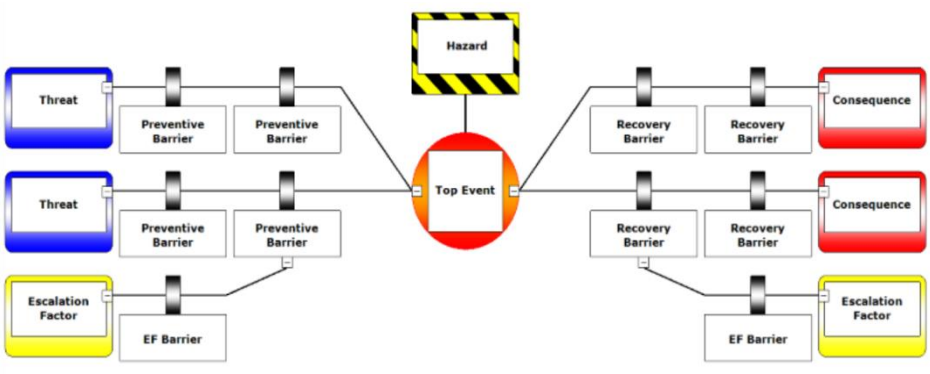

Figure 1. Typical bow-tie diagram (Merrett et al., 2019).

3.1. Full Consistency Method Integrated with Fuzzy (FUCOM-F)

In this section, firstly, triangular fuzzy numbers (TFNs) and their mathematical operations are defined in detail. Then, the purpose and steps of FUCOM are identified. For FUCOM-F, the linear problem, which is the last algorithm of FUCOM, is solved by considering TFN's operations.

3.1.1. Triangular fuzzy numbers

The linguistic variables are assigned to membership degrees via fuzzy set theory. There are several types of fuzzy numbers, such as triangular, trapezoidal, picture, but the most frequently used fuzzy numbers are TFN in the literature (Ecer, 2014). The outlines of fuzzy sets and operations of TFN are briefly defined below (Pamucar & Ecer, 2020).

Theorem 1: A special fuzzy set $\{(x, \mu_F(x)), x \epsilon R\}$ is called a fuzzy number, where $\mu_F(x)$ is a membership function in the defined interval [0,1], and *x* has its values on the real line, R: $\infty \leq x \leq \infty$

Theorem 2: A TFN represents the relative dominance of each pair of factors in the same hierarchy, and can be demonstrated as T = (l, m, n), where $l \leq m \leq n$. l, m, and n parameters show the lower bound value, the centre, and the upper bound value in a fuzzy event, respectively. In Eq. (1), triangular type of membership function of T fuzzy number is identified.

$$\mu_T(x) = \begin{cases} 0, & x < 1 \\ (x-l)/(m-l), & l \leq x \leq m \\ \frac{n-x}{n-m}, & m \leq x \leq n \\ 0, & x > n \end{cases} \quad (1)$$

When there are two TFNs as T_1= (l_1, m_1, n_1) and T_2=(l_2, m_2, n_2), the main operations of two fuzzy numbers are as in the following equations:

$$(l_1, m_1, n_1) \oplus (l_2, m_2, n_2) = (l_1 + l_2, m_1 + m_2, n_1 + n_2) \quad (2)$$

$$(l_1, m_1, n_1) \otimes (l_2, m_2, n_2) = (l_1 l_2, m_1 m_2, n_1 n_2) \quad (3)$$

$$(l_1, m_1, n_1) / (l_2, m_2, n_2) \cong (l_1/n_2, m_1/m_2, n_1/l_2) \; for \; l_i > 0, m_i > 0, n_i > 0 \quad (4)$$

$$(l_i, m_i, n_i)^{-1} \approx \left(\frac{1}{n_i} \frac{1}{m_i} \frac{1}{l_i}\right) \; for \; l_i > 0, m_i > 0, n_i > 0 \quad (5)$$

Theorem 3: The graded mean integration representation (GMIR)

Consider $\alpha_j = (l_j, m_j, n_j)$ as a TFN and GMIR R (α_j)of α_j are calculated as:

$$R(\alpha_j) = \frac{l_j + 4m_j + n_j}{6} \quad (6)$$

3.1.2. Fuzzy FUCOM (FUCOM-F)

The FUCOM-F method is offered by Pamucar and Ecer (2020) for weightng the importance of the criteria in a MCDM system. Accordingly, n evaluation criteria, which are denoted as w_j, j = 1,2, ...,n, are assumed in a MCDM issue, and their importance weight coefficients are required to be understood. For determining the impact level of criterion i on criterion j (a_{ij}), pairwise comparisons of criteria are created through expert opinions. In the evaluation models by experts, uncertainties generally exist for the assessment of criteria. In this case, the application of fuzzy numbers in MCDM systems is most frequently preferred. For this purpose, a fuzzy linguistic scale in Table 1, which is described by TFNs, is used to present expert opinions in the FUCOM-F.

Linguistic terms	Membership function
Equally important (EI)	(1,1,1)
Weakly important (WI)	(2/3,1,3/2)
Fairly Important (FI)	(3/2,2,5/2)
Very important (VI)	(5/2,3,7/2)
Absolutely important	(7/2,4,9/2)

Table 1. Fuzzy linguistic scale (Pamucan and Ecer, 2020)

Pamucar and Ecer (2020) extended the basic function of the traditional FUCOM in the fuzzy environment and forwarded the FUCOM-F algorithm, as shown in the flow diagram in Figure 2. According to the algorithm of FUCOM-F, the weights of the coefficient of criteria are found by solving a linear problem, as shown in the last step in Figure 2. Accordingly, the minimum DMC, i.e., X=0, is satisfied only if the transitivity among weight coefficients is completely satisfied. It is necessary to determine the values of the weight coefficients of criteria that satisfy the conditions, which are shown in Figure 2, with the minimisation of value X.

The FUCOM methodology consists of several advantages. FUCOM has an easy implementation algorithm. The method makes it possible to get trustworthy weight coefficients, which aid in rational judgment and lead to believable decision-making outcomes. FUCOM is a tool that, by means of an appropriate scale and a straightforward algorithm, assists executives in dealing with their inherent subjectivity when it comes to prioritising criteria. By using a simple mathematical tool and the FUCOM model, you can find the best values for the weight coefficients that allow you to favour certain criteria when judging phenomena based on the needs of the decision-maker at the time and with the least amount of risk. Furthermore, FUCOM gives the best values for the weight coefficients and makes the experts' preferences less influential and inconsistent with the final criterion weight values. Based on these aspects, the FUCOM-F methodology is selected to prioritise the importance of ECDIS cyber security.

Step 1

- Define evaluation criteria for MCDM problem.
- n (j=1,2,...,n) evaluation criteria that are represented by a set C={C1, C2, ….Cn}.

Step 2

- Rank the decision criteria.
- Experts determine the rank of criteria in accordance with their preferences regarding the significance of the criteria
- The first rank is assigned to a criterion that is expected to have the highest weight coefficient and so on, towards the criterion of the least significance by the experst.
- Cj(1) > Cj(2) > Cj(k) , k is the rank of the criterion observed

Step 3

- Comparisons of the criteria using TFNs.
- The comparison is made with respect to the first-ranked (most significant) criterion by using values in Table 3.
- The fuzzy criterion significance $\bar{w}(C_{j(k)})$
- Since the first-ranked criterion is compared with itself (its significance is $\bar{w}(C_{j(k)})$=EI), n-1 comparison of the remaining criteria must be performed.
- For obtaining fuzzy comparative significance, the following equation is used:
- $\varphi_{k/(k+1)} = \frac{\bar{w}(C_{j(k+1)})}{\bar{w}(C_{j(k)})} = \frac{\bar{w}(C_{j(k+1)})^l, \bar{w}(C_{j(k+1)})^m, \bar{w}(C_{j(k+1)})^n}{\bar{w}(C_{j(k)})^l, \bar{w}(C_{j(k)})^m, \bar{w}(C_{j(k)})^n}$

Step 4

- Calculate the optimal fuzzy weight coefficients of criteria (w1, w2,...,wn)T.
- The final values of weight coefficients should satisfy two conditions:

Step 4.1

- Condition 1: $\frac{w_k}{w_{k+1}} = \varphi_{k/(k+1)}$
- Condition 2: $\frac{w_k}{w_{k+2}} = \varphi_{k/k+1} \otimes \varphi_{(k+1)/(k+2)}$

Step 4.2

- set the final nonlinear model for determining the optimal fuzzy values of the weight coefficients of the evaluation criteria (w1, w2,...,wn) according to the defined conditions in step 4.1.
- Min χ
- s.t.

$$\begin{cases} \left|\frac{w_k}{w_{k+1}} - \varphi_{k/(k+1)}\right| \le \chi, \forall_j \\ \left|\frac{w_k}{w_{k+2}} - \varphi_{k/k+1} \otimes \varphi_{(k+1)/(k+2)}\right| \le \chi, \forall_j \\ \sum_{j=1}^{n} w_j = 1, \ \forall_j \\ w_j^l \le w_j^m \le w_j^n \\ w_j^l \ge 0, \forall_j, \quad j = 1,2,\dots,n \end{cases}$$

- where $w_j = w_j^l, w_j^m, w_j^n$ and $\varphi_{k/(k+1)} = (\varphi_{k/(k+1)}{}^l, \varphi_{k/(k+1)}{}^m, \varphi_{k/(k+1)}{}^n)$.

Step 4.3

- In order to achieve the highest consistency, it is necessary to satisfy the condition that $\frac{w_k}{w_{k+1}} - \varphi_{k/(k+1)} = 0$ and $\frac{w_k}{w_{k+2}} - \varphi_{k/k+1} \otimes \varphi_{(k+1)/(k+2)} = 0$
- Thereby, the model given in step 4.2 can be transformed into a fuzzy linear model as below. The optimal fuzzy values of weight coefficients are obtained (w1, w2,...,wn)T, if it is solved.

- Min χ
- s.t.

$$\begin{cases} \left|w_k - w_{k+1} \otimes \varphi_{k/(k+1)}\right| \le \chi, \forall_j \\ \left|w_k - w_{k+2} \otimes \varphi_{k/(k+1)} \quad \otimes \varphi_{(k+1)/(k+2)}\right| \le \chi, \forall_j \\ \sum_{j=1}^{n} w_j = 1, \ \forall_j \\ w_j^l \le w_j^m \le w_j^n \\ w_j^l \ge 0, \forall_j, \quad j = 1,2,\dots,n \end{cases}$$

- where $w_j = w_j^l, w_j^m, w_j^n$ and $\varphi_{k/(k+1)} = (\varphi_{k/(k+1)}{}^l, \varphi_{k/(k+1)}{}^m, \varphi_{k/(k+1)}{}^n)$.

Figure 2. Flow diagram for FUCOM-F method.

4. APPLICATION

4.1. Identifying ECDIS Cyber Security Dynamics

For the FUCOM-F method, it is required to create related criteria as a hierarchical table. The sources mentioned in Section 3 (the technological standards and qualifications of ECDIS, the ECDIS operational handbook, the ECDIS standard type approval certificate, ECDIS manufacturers' catalogues, ITU standards, and the DNV-GL guideline) are utilised for creating a criteria table for ECDIS cyber security, including threats, barriers, mitigation, and consequences. Accordingly, the dynamics for ECDIS cyber security are as in Tables 2 and 3. In these tables, cyber threats and consequences related to ECDIS are the main criteria, while the barriers and mitigations related to the cyber security of ECDIS are designed as sub-criteria for threats and consequences, respectively. After obtaining the importance weights of each of these factors and sequencing them orderly via FUCOM-F, a model related to cyber security in ECDIS, according to the importance weights of these factors, is formed through the bow-tie model.

Criteria (Threats)	Number	Sub criteria (Barriers)	
Malware infection via internet and intranet (M1)	G1	Up-to-date virus protection and scanning software	Protection against malware (M11)
	G2	Up-to-date information and technological (IT) systems (update operating system, etc.)	
	G3	Documentation and monitoring of changes made to an existing IT system	
	Z1	Security system and software update procedures for ECDIS	Security Management (M12)
	Z2	Procedures on ECDIS for areas where the human factor is important	
	Z3	Training procedures on ECDIS cyber security of ship personnel	
	Z4	Procedures for regular password change	
	Z5	Adoption of existing standards and rules that will contribute to ECDIS cyber security, such as ISO/IEC 27001	
Introduction of malware on removable media (M2)	F1	Closing ECDIS USB ports	
	F2	Using a single, fixed external memory for ECDIS	
	F3	Pre-scan of external memory to be used in ECDIS	
Intrusion via remote access (M3)	T1	Whitelisting of systems previously authorised for remote connection to ECDIS	

	T2	Using a secure network (VPN) using appropriate encryption methods during remote access to maintain or troubleshoot ECDIS
	T3	Authentication access procedure
Vulnerabilities of standard components of IT systems and other control systems connected to the internet (M4)	S1	All foundations of the system, from the network topology to the after-service requirements, during the procurement and placement of the systems integrated with ECDIS, by authorised, licensed parties
	S2	Restricting the connection of systems with each other via the Internet or communication with each other
	S3	Physical security - setting up environmental controls around secure and controlled locations
	S4	Operating systems - patch management and locked out of access to firmware
	S5	Applications - creating rules for software installation and default configurations
	S6	Security tools - distributing anti-virus and reporting any endpoint protection appropriately
	S7	Networks and services - removing unnecessary services (eg. Telnet, ftp) and enabling secure protocols (eg. Ssh, sftp)
	S8	Access control - make sure default accounts are renamed or disabled
	S9	Data encryption - encryption keys to use (eg. SHA-256)
	S10	System backup - correct configuration of backups
Human error and sabotage (M5)	C1	Systematic staff training on information security, authorised access system, administrator and user rights
	C2	Compliance management system with predetermined rules, procedures and standards
	C3	Cyber Incident reporting system

Table 2. ECDIS cyber threats and their barriers

Criteria (Consequences)	Number	Sub criteria (Mitigations)
System is unavailable (O1)	B1	Network segregation
	B2	Network traffic information collection
	B3	Machine-readable reporting of current security settings
System is corrupted (O2)	D1	System architecture and isolation mechanisms preventing spreading of viruses, malware, etc.
	D2	Disaster recovery procedures
	D3	Software fault tolerance
	D4	Control system recovery and reconstitution
Files in ECDIS are deleted or changed (O3)	E1	Data protection against information theft
	E2	Backup procedures and regular testing of backups
	E3	Cryptology
	E4	Patch and change management
Other devices connected with ECDIS, such as GPS, AIS etc.. are hijacked (O4)	H1	Physical Network Segmentation
	H2	Logical network segmentation
	H3	Secure communication
Infrastructure is damaged (O5)	J1	Adequately managed outsourcing of IT/OT responsibilities or services
	J2	Incident handling routines
	J3	Business continuity management

Table 3. ECDIS cyber consequences and their mitigations

4.2. Data Collection

In this study five expert opinions are used for FUCOM-F methods. The selection of experts is based on NIST's definition of cyber security. According to NIST (2023), cybersecurity is the act of safeguarding, mitigating harm to, and recovering electronic communication services and systems. This encompasses the data held within these systems, which cybersecurity experts strive to safeguard. Cybersecurity encompasses all aspects related to electronic systems and communications. Subcategories exist within the area of cybersecurity, each requiring additional specialisation. These encompass security measures for cloud computing, network, and critical infrastructure security. Consequently, this study made sure to select experts with diverse backgrounds in information security, such as information processing, security, software development, etc., to determine the importance of measures related to ECDIS cyber security. ECDIS, while classified as an information technology, is also recognised as an operational technology because it is integrated with other operational technologies on the ship's bridge, particularly with serial and network data transfer. Therefore, an expert with expertise in marine cyberspace, familiarity with maritime communication protocols, and understanding of the vulnerabilities and safeguards associated with data transmission in these protocols, has also been added. The demographic information of experts is as shown in Table 4.

Experts scored using the scale system in the range of 1-9, regarding the pairwise comparison of the criteria and sub-criteria in Table 2 and Table 3, according to the importance level. The arithmetic means of expert scores, given during the pairwise comparison, are calculated to obtain the final scores for use in the steps of the FUCOM-F methods.

Experts	Occupation	Experience
EXP1	Manager in the Information Systems Department, software development and control engineer, system engineer, wireless communication solutions in various company related maritime	18 years
EXP2	Software Engineering in maritime	5 years
EXP3	Computer Engineering	9 years
EXP4	Information and Data Security Executive	12 years
EXP5	Academician on Maritime Cyber Security	3 years

Table 4. Demographic information of experts

4.3. Analysis of ECDIS Cyber Security via FUCOM-F Method

For evaluating the importance weights of the cyber security dynamics related to ECDIS, two stages of application for FUCOM-F are performed. The first stage includes determining the importance of cyber threats and the consequences related to ECDIS. In the second stage, the importance of barriers for threats and mitigations for consequences are determined. The purpose of the FUCOM-F approach is to define the connected values of weight coefficients for the first and second-level criteria. After the importance weights of the sub-criteria, representing barriers and mitigations, are obtained, these values are multiplied by the corresponding importance weights of the threats and consequences respectively. Thereby the global optimal weights of barriers and mitigations are revealed.

The steps of the FUCOM-F method in Figure 2 are applied by considering each experts' scores separately. The arithmetic mean of the obtained results from these process is taken for achieving the final criteria weights. All equations for the FUCOM-F are defined in the Excel programme, and the linear problem is solved in the programme for all factors separately.

Firstly, according to expert scores for pairwise comparisons of cyber dynamics related to ECDIS, considered dynamics are ranked. Subsequently, the 1-9 scaled ranking scores are transformed into fuzzy linguistic scales. Finally, they are transformed into triangular fuzzy numbers (TFN) by referencing Table 1.

The method is illustrated by considering a barrier and its sub-criteria. According to expert 1 scores, the sub-barriers (G matrix) of protection against malware (M11) are ranked as follows:

EXP1: G1>G2>G3

In the following step, according to the opinion of Expert 1 (EXP1), the linguistic variables of the comparative significance of the criteria ranked are defined as in Table 5.

Barriers	G1	G2	G3
Linguistic variables	EI	EI	WI

Table 5. Linguistic evaluations of barrier G_i

The TFN transformation of linguistic variables is performed by using the fuzzy linguistic scale in Table 1. The transformation result for n the G_i barrier is as shown in Table 6.

Barriers	G1	G2	G3
Linguistic variables	(1,1,1)	(1,1,1)	(2/3,1,3/2)

Table 6. TFN transformation of evaluations

In this step, the comparative significance of the criteria is obtained by using the equation in step 3 in Figure 2 as follows:

$\varphi_{G1/G2}= \frac{\bar{w}_{G_1}}{\bar{w}_{G_2}}$ = (1,1,1) /(1,1,1)= (1,1,1)

$\varphi_{G2/G3}= \frac{\bar{w}_{G_2}}{\bar{w}_{G_3}}$ = (2/3,1,3/2) /(1,1,1)= (0.67,1,1.5)

According to the comparative significance of the criteria, the vector of comparative significance is revealed as $\emptyset = ((1,1,1), (0.67,1,1.5))$. Then, the constraints of the analysis for matrix of G_i barrier are identified. According to the expressions in step 4.1 in Figure 2, the first group of constraints are $\frac{w_{G1}}{w_{G2}} = (1,1,1)$ and $\frac{w_{G2}}{w_{G3}} = (0.67,1,1.5)$ and the second group of constraints are $\frac{w_{G1}}{w_{G3}} = (1,1,1).(0.67,1,1.5) = (0.67,1,1.5)$. Based on the defined constraints, a linear model according to step 4.3 in Figure 2 is formed for determining the optimal values of the weight coefficients of dimensions.

By solving the linear problems model, the optimum values of the weight coefficients of G_i:

W_{Gi} =((0.3303, 0.3303, 0.3303), (0.3303, 0.3303, 0.3303), (0.2202, 0.3303, 0.4954))

and χ =0.000 are obtained.

The same steps have also been applied for the main cyber threats (M matrix). Then, the obtained local fuzzy values of M1 threat weight coefficients are multiplied by the barriers of the G matrix to achieve global fuzzy values of the G matrix weight coefficients. The barriers are related to threats; therefore, the weight coefficients of threats are important for barriers. Similarly, the same thought applies to mitigations and consequences in this study.

W_{M1} = (0.2217, 0.2217, 0.2217)

Global W_{Gi}= W_{Gi}*W_{M1}=((0.7321, 0.7321, 0.7321), (0.7321, 0.7321, 0.7321), (0.4881, 0.7321, 0.1098))

Finally, the defuzzification transformation (DT), which is stated in the study of Kayalvizhi et al. (2016), is applied to the fuzzy values of the weight coefficients of factors to obtain crisp values as follows:

DT = (l+2m+n)/4

Accordingly, the crisp values of G_i weight coefficients are obtained as follows:

DT(G_i) = (0.073, 0.073, 0.076)

All these steps are applied to each threat, barrier, mitigation, and consequence. At the end of the process, the fuzzy local weight coefficients of each barrier are multiplied by the fuzzy local weight coefficients of the related threat. Similarly, the fuzzy local weight coefficients of each mitigation are

multiplied by the fuzzy local weight coefficients of the related consequence. Then, all fuzzy values of weight coefficients are transformed into crisp values. After the process is applied to the scores of each expert separately, the arithmetic mean of the obtained crisp values of factors is taken. Consequently, the related results of each step are listed in the supplementary files. In this study, the method applied is verified over only one factor for sampling.

4.4. Findings

As a result, the obtained results from the FUCOM-F method are shown in Tables 7 and 8. The DT (G_i) values of EXP 1, which have been shown in the above section, are also shown in the second column, where they correspond to row G in Table 7. After the above-mentioned process of the methodology is applied for each dynamics, the final weight coefficients are as in the “Mean” column.

Criteria	EXP1	EXP2	EXP3	EXP4	EXP5	Mean
M1	0,222	1,666	0,175	0,256	0,213	0,506
M2	0,115	0,206	0,210	0,205	0,210	0,189
M3	0,222	0,220	0,213	0,123	0,175	0,191
M4	0,115	0,200	0,154	0,199	0,171	0,168
M5	0,222	0,172	0,171	0,134	0,154	0,170
G1	0,073	0,080	0,081	0,096	0,098	0,086
G2	0,073	0,049	0,074	0,087	0,090	0,075
G3	0,076	0,088	0,029	0,025	0,043	0,052
Z1	0,058	0,056	0,044	0,084	0,041	0,057
Z2	0,035	0,052	0,043	0,029	0,023	0,036
Z3	0,032	0,030	0,034	0,031	0,038	0,033
Z4	0,057	0,025	0,020	0,025	0,030	0,031
Z5	0,028	0,044	0,036	0,031	0,046	0,037
F1	0,074	0,092	0,030	0,088	0,077	0,072
F2	0,019	0,107	0,068	0,023	0,093	0,062
F3	0,024	0,032	0,123	0,028	0,067	0,055
T1	0,025	0,035	0,105	0,070	0,055	0,058
T2	0,098	0,066	0,026	0,033	0,055	0,056
T3	0,098	0,066	0,027	0,025	0,049	0,053
S1	0,107	0,025	0,101	0,127	0,106	0,093
S2	0,026	0,081	0,057	0,110	0,101	0,075
S3	0,027	0,070	0,072	0,086	0,080	0,067
S4	0,029	0,053	0,086	0,104	0,086	0,072
S5	0,029	0,095	0,027	0,121	0,057	0,066
S6	0,043	0,050	0,106	0,033	0,027	0,052
S7	0,059	0,024	0,086	0,104	0,086	0,072
S8	0,074	0,027	0,029	0,035	0,029	0,039
S9	0,104	0,040	0,043	0,051	0,043	0,056
S10	0,089	0,027	0,029	0,035	0,029	0,042
C1	0,083	0,057	0,074	0,080	0,056	0,070
C2	0,071	0,055	0,072	0,043	0,061	0,060
C3	0,073	0,064	0,026	0,082	0,054	0,060

Table 7. The results of FUCOM-F for threats and barriers

Criteria	EXP1	EXP2	EXP3	EXP4	EXP5	Mean
O1	0,105	0,219	0,373	0,263	0,219	0,236
O2	0,143	0,255	0,178	0,259	0,184	0,204
O3	0,192	0,241	0,176	0,127	0,198	0,186
O4	0,300	0,118	0,135	0,145	0,115	0,162
O5	0,130	0,194	0,100	0,157	0,241	0,164
B1	0,032	0,050	0,034	0,089	0,041	0,049
B2	0,047	0,055	0,043	0,043	0,049	0,047
B3	0,047	0,048	0,039	0,031	0,037	0,040
D1	0,022	0,053	0,029	0,044	0,053	0,040
D2	0,079	0,029	0,037	0,047	0,056	0,050
D3	0,020	0,056	0,039	0,036	0,029	0,036
D4	0,025	0,045	0,035	0,028	0,049	0,037
E1	0,075	0,033	0,044	0,044	0,073	0,054
E2	0,019	0,087	0,036	0,057	0,059	0,051
E3	0,024	0,031	0,048	0,039	0,039	0,036
E4	0,059	0,056	0,047	0,022	0,067	0,050
H1	0,065	0,051	0,151	0,043	0,088	0,079
H2	0,168	0,092	0,119	0,121	0,076	0,115
H3	0,183	0,085	0,129	0,110	0,070	0,115
J1	0,084	0,033	0,070	0,065	0,085	0,067
J2	0,027	0,092	0,061	0,036	0,068	0,057
J3	0,022	0,083	0,056	0,031	0,077	0,054

Table 8. The results of FUCOM-F for consequences and mitigations

Examining the column of criteria weights in Table 7, it may be seen that the most important main cyber threat for ECDIS is malware infection via the internet and intranet (M1). Then the order of importance of the main cyber threats for ECDIS is as follows: the introduction of malware on removable media (M2), intrusion via remote access (M3), vulnerabilities of standard components of IT systems and other control systems connected to the internet (M4), and human error and sabotage (M5) respectively.

From Table 7 it may be understood that the most important barriers for M1 threats are up-to-date virus protection and scanning software (G1), which is a sub-barrier of protection against malware (M11). This is followed by up-to-date information and technological (IT) systems (update operating system, etc.) (G2), and documentation and monitoring of changes made to an existing IT system (G3) for M11 barriers. The security system and software update procedures for ECDIS (Z1) are the most important barriers for M1 threats among security management (M12) sub-barriers. This is followed by procedures on ECDIS for areas where the human factor is important (Z2), adoption of the existing standards and rules that will contribute towards ECDIS cyber security, such as ISO/IEC 27001 (Z5), training procedures on ECDIS cyber security for ship personnel (Z3), and procedures for regular password change (Z4) respectively.

Upon examining Table 8 it may be noticed that the most important potential consequence if these cyber threats related to ECDIS cannot be prevented is “system is unavailable (O1).” The second potential consequence is “system is corrupted (O2)”. In the third rank for significant potential consequences, there are consequences of “files in ECDIS are deleted or changed (O3)” and “infrastructure is damaged (O5)”, with the same criteria weights. The last potential consequence is “other devices connected with ECDIS, such as GPS, AIS etc., are hijacked (O4)”.

According to the results, the most critical mitigation to prevent the consequence of O1 is network segregation (B1). Then the network traffic information collection (B2) and machine-readable reporting of current security settings (B3) are to follow it.

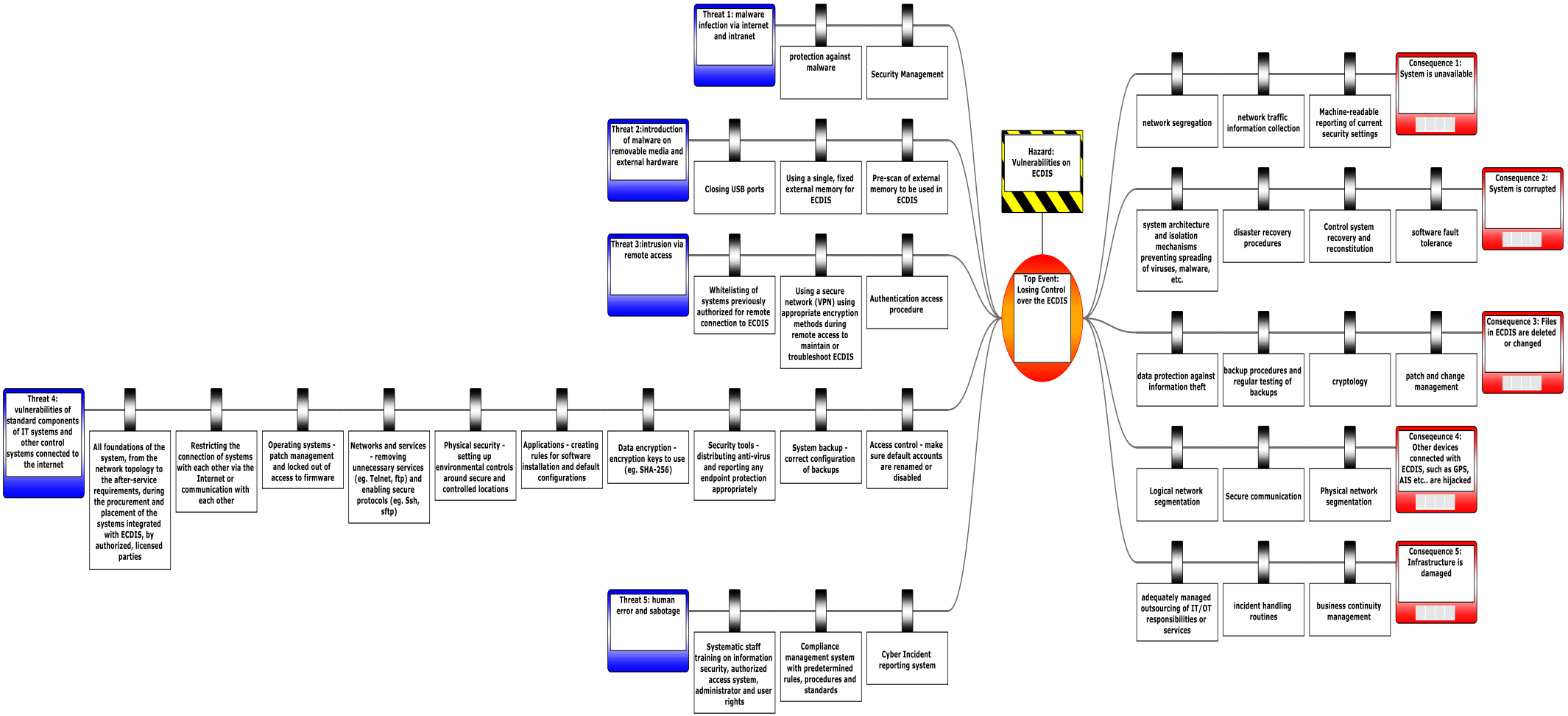

Figure 3. Bow-tie diagram for cyber security of ECDIS.

4.5. Bow- Tie Analysis for Cyber Security of ECDIS

According to the hierarchical level obtained for the ECDIS cyber security model, the bow tie model is created, as shown in Figure 3. The holistic view of ECDIS cyber security, which includes cyber threats, IT and OT dynamics, and consequences, is presented as a model

5. DISCUSSION

In this study the dynamics constituting ECDIS cyber security have been are analysed and prioritised with a holistic approach, and a hierarchical system has been obtained accordingly. With the hierarchical system presented in Figure 3, it is envisaged that ECDIS cyber security will be provided at a high level of convergence at the technical level. The hierarchical model obtained in this context can be a guide for ship officers who are responsible for ECDIS cyber security, company managers, and even insurers in any cyber incident, to make policy on the proposed hierarchical diagram. Company managers, particularly, can strategically invest in cyber security, including ECDIS, by thoroughly analysing the hierarchical model.

On the other hand, it is important to state that "uncertainties" are inevitable in all scientific endeavours, especially in MCDM, and cannot be circumvented. The quantification and expression of uncertainties in data and analysis are contingent upon the methodologies employed in scientific research (Montewka et al. 2014; Berner & Flage, 2016). The research highlights the challenge of calculating expert opinion of criteria in maritime transportation due to a scarcity of data, potentially leading to ambiguity. Data scarcity primarily arises from physical limitations or insufficient resources. Expert elicitation is the process of combining the opinions of experts on a subject when there is uncertainty because of a lack of data (Rausand and Hoyland, 2004). Experts' elicitation is an approach that relies on scientific consensus. It enables the incorporation of parameters, which are actually "informed estimations", to analyse the specific subject being investigated, as it may measure the level of uncertainty.

Upon examining the data presented in Figure 3, it is clear that the threats and their consequences that pose a risk to ECDIS cyber security are organised in a hierarchical fashion. The most significant threats and consequences are listed at the top, while the most significant barriers and mitigations are listed from left to right, based on their respective levels of influence on the diagram. The ECDIS cyber security faces multiple challenges, with the most effective defense against each attack being the far-left.

The most prominent risk to ECDIS cyber security is the infiltration of malware through both the internet and intranet. Malicious software, such as Trojans, viruses, spyware, ransomware, adware, rootkits, and worms, have the ability to infiltrate computer systems, compromising data and causing harm. In order to mitigate malware infections, it is imperative to utilise up-to-date malware protection and scanning software on information technology systems. Maintaining the latest updates on self-owned computers is the most efficient measure to prevent malware infiltration according to the analysis results. Additionally, it is necessary to ensure that any IT systems employed on board are regularly updated and remain valid, serving as an additional layer of protection. Thoroughly documenting and closely monitoring any modifications made to current IT systems are essential in order to systematically thwart the infiltration of malicious software. Implementing security management measures on board is crucial for preventing malware as the next barrier on the diagram. This encompasses the tasks of formulating and executing comprehensive security protocols, overseeing the enforcement of these protocols, upgrading security infrastructure and software, complying with international standards like ISO/IEC 27001, providing training to ship staff, and conducting periodic password modifications. The management system should prioritise proactive measures over reactive ones, aiming to mitigate hazards before they become manifest.

From the analysis results, it may be understood that remote access intrusion poses significant risks on the ECDIS after the infiltration of malware, as IT staff often need remote maintenance access to the ship instead

of physically going for prompt reaction or support. All systems used on board for communication with shore for any reason, such as operation, positioning, etc., are vulnerable to interference, as seen in reported incidents in maritime history. In addition, especially ECDIS navigation chart updates are realised over the internet. In such cases, unauthorised remote access can reveal if required barriers are not taken. Such threats can be eliminated or their risks decreased when the proper proactive prevention processes are carried out. Remote access management can mitigate such breaches by allowing users to access the system with predefined rights, employing whitelisting, and ensuring safe data transmission over a protected network, using robust encryption techniques. Enforcing the use of an encrypting virtual private network (VPN) should be mandatory if remote access is permitted. A policy for securing remote access should be established for all parties involved, and a mechanism for authentication access should be developed for groups such as companies, IT staff, service providers, or maintenance teams.

The third and lower level cyber threats for ECDIS and their barriers are summarised as follows. The potential for malware infiltration through removable media and other hardware is likewise a matter of worry. To mitigate these risks, it is essential to disable USB ports, use a single, stationary external memory for ECDIS, and perform a preliminary scan of the external memory. Additionally, a single encrypted USB device should be allowed for routine tasks within the central control station of the entire ship. In continuation, ships face significant cyber security risks due to the complex nature of the cyber environment, including network topology, electronic systems, operational and monitoring systems, cyber physical systems, and information systems. In order to tackle this problem, it is necessary to provide comprehensive and structured training for both ship and company staffs, as well as individuals involved in the ship's supply chain. A cyber security management system (CMS) can help mitigate cyber risks caused by human error and sabotage by assessing and tracking actions within an organisation based on established rules, regulations, procedures, and standards. Internet-connected control components pose a lower risk to ECDIS cybersecurity, but all aspects of these systems must be carried out exclusively by approved and licensed entities.

If every associated threat manages to bypass all the established barriers in the analysis, then the consequences that affect ECDIS functions may occur as can be seen from the study findings. The most significant outcome of breaching ECDIS cybersecurity is the unavailability of the system. System availability is the proportion of the total time that services and software applications on servers are accessible to clients, barring emergency repairs, regular maintenance periods, or user actions that result in system downtime. Ransomware can disrupt system availability by propagating through drivers, connected PCs, servers, or other accessible devices linked to the network. Measures to protect against ransomware encompass network segmentation, gathering network traffic data, and generating machine-readable reports on existing security configurations. The machine-readable format is mainly related to Common Industrial Protocol (CIP) Security. CIP Security includes IP Security Ether Net / IP Confidentiality Profile and CIP Security User Authentication Profile. ISA/IEC 62443 is a standard which addresses the point on cyber security in industrial control systems. The machine-readable reporting of current security settings is one of the component-level requirements of each IEC 62443-4-2, showing the related CIP Security functionality that covers the requirement.

The second severe consequence of ECDIS cyber security is system corruption, where malware can infiltrate the system via exploiting vulnerabilities in the network, accessing network shares, deceiving users with corrupted files, or distributing copies of itself or other malware to users. Systems are deemed corrupted when they have been compromised. To prevent system corruption, the order of prevention should be disaster recovery procedures, system architecture, isolation mechanisms, information system recovery and reconstitution, as well as the software fault tolerance. Disaster recovery procedures involve creating an IT inventory, defining assets, vulnerabilities, and risks, and establishing a recovery timeline. System architecture and isolation mechanisms include computer security programs, such as run-time virus control, antivirus programs, firewalls, secure networks, backup systems, and encryption. Software fault tolerance guarantees the

uninterrupted operation of a system, even if one or more of its components should fail, hence ensuring the preservation of confidentiality, integrity, and availability.

The third level most important consequences for ECDIS is file deletion or change. To prevent this, the most effective mitigation is "logical network segmentation". If insufficient, "secure communication" should be applied, and the least effective is "physical network segmentation". Cyberattacks can capture, delete, or change files without data protection, leading to data theft. The steps to protect critical information, backup procedures, patch and change management, and encrypting files should be implemented. Sensitive information should be restricted, removed from online databases or clouds, and encrypted during transfer or e-mailing.

Lastly, for the consequences related to infrastructure damage, manufacturing operations management covers various IT and OT processes as outsourced services, divided into service operations and service planning. These processes provide performance and cost visibility, making it easier to control IT and OT services. IT governance and organizations should agree on definitions of key performance indicators and measurement methods. Although providing separate or integrated outsourced IT and OT services is costly and hard to interconnect for maritime, having such a resource procures well-managed outsourced IT and OT responsibilities or services, incident handling routines, and business continuity management, respectively.

6. CONCLUSION

In this study, the importance weights of ECDIS cyber dynamics are obtained. In this context, the threats and consequences related to the loss of control of ECDIS are defined, and their barriers and mitigations are tried to be developed. Thereby the importance weights of threats, consequences, barriers, and mitigations on the cyber security of ECDIS are found via FUCOM-F methods. As a result, a bow-tie model has been developed in order to demonstrate a holistic view, in accordance with the hierarchical ranking of the dynamics.

For weighing the importance of dynamics, FUCOM integrated with fuzzy methods is used. FUCOM-F is considered to be an easier and more effective method for defining the importance of criteria, better than other criteria weighing methodologies in the literature, because it requires a smaller number of expert comparisons. Fuzzy set theory is used with FUCOM to deal with the abstruseness and ambiguity problems in expert decisions. It provides the best expression for causing structure and human consideration, as well as more reliable and valid results.

The results of this study provide an insight into ensuring overall ECDIS cyber security onboard ships. The International Maritime Organisation (IMO) requires that all ships complying with SOLAS must include the cyber security clause in their safety management system. Shipping companies need a consultancy to create an efficient cyber security management system for their ships. From this point of view, this study provides detailed guidelines for shipping companies and other maritime stakeholders in terms of adopting a methodology for cyber security investment and improvement.

For further studies, it is considered that the importance weights obtained for IT and OT dynamics, related to the cyber security of ships, should be identified separately for considering other cyberspaces of ships, such as RADAR, GPS, AIS, etc. Consequently, the importance of the cyber security of ships can be obtained timely. For this purpose, while the same method can be used, state-of-the-art methods, such as artificial neural networks and Bayesian networks, can be used.

The number of experts (5) can be considered a limitation of the study, even though they are experienced in cyber security and information and operational technologies. However, both the number of experts and their qualifications can be improved in further studies. Additionally, the uncertainties and bias cannot be eliminated due to the lack of statistical data in this study.

ACKNOWLEDGEMENT

This study is supported by the Istanbul Technical University - Scientific Research Projects -General Research Project – “ECDIS Cyber Security Penetration Test Application and Analysis” [Project ID: 44740].

This study is supported by the Research Team of Istanbul Technical University, Maritime Faculty, Maritime Security and Cyber Threats Research Laboratory, Türkiye.

CONFLICT OF INTEREST STATEMENT

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

REFERENCES

Abdullah, A. et al. 2022. Healthcare Performance Management Using Integrated FUCOM-MARCOS Approach: The Case of India. The International Journal of Health Planning and Management, 37(5), pp. 2635-2668. Available at: https://doi.org/10.1002/hpm.3488.

Alekseenkov, A. et al. 2021. Cyberattacks in the Water Transport Industry: Types and Diversity. In International Scientific Siberian Transport Forum, pp. 1532-1540.

Amro, A. & Gkioulos, V. 2023. Evaluation of a Cyber Risk Assessment Approach for Cyber–Physical Systems: Maritime-and Energy-Use Cases. Journal of Marine Science and Engineering, 11(4), p. 744. Available at: https://doi.org/10.3390/jmse11040744.

Androjna, A. et al. 2020. Assessing Cyber Challenges of Maritime Navigation. Journal of Marine Science and Engineering, 8(10), p. 776. Available at: https://doi.org/10.3390/jmse8100776.

Badi, I. & Abdulshahed, A. 2019. Ranking the Libyan Airlines by Using Full Consistency Method (FUCOM) and Analytical Hierarchy Process (AHP). Operational Research in Engineering Sciences: Theory and Applications, 2(1), pp. 1-14. Available at: https://doi.org/10.31181/oresta1901001b.

Badi, I. et al. 2022. Measuring Sustainability Performance Indicators Using FUCOM-MARCOS Methods. Operational Research in Engineering Sciences: Theory and Applications, 5(2), pp. 99-116. Available at: https://doi.org/10.31181/oresta040722060b.

Ben Farah, M. A. et al. 2022. Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. Information, 13(1), 22.

BIMCO. 2020. The Guidelines on Cyber Security Onboard Ships - Version 4. Available at: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Bolbot, V. et al. 2020. A Novel Cyber-Risk Assessment Method for Ship Systems. Safety science, 131, 104908. Available at: https://doi.org/10.1016/j.ssci.2020.104908.

DNV-GL. 2016. Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation. DNVGL-RP-0496, Edition September: 1–86. Available at: https://www.gard.no/Content/21865536/DNVGL-RP-0496.pdf

Ecer, F. 2014. A Hybrid Banking Websites Quality Evaluation Model Using AHP and COPRAS-G: A Turkey Case. Technological and Economic Development of Economy, 20(4), pp. 758-782.

Erceg, Ž. & Mularifović, F. 2019. Integrated MCDM Model for Processes Optimization in Supply Chain Management in Wood Company. Operational Research in Engineering Sciences: Theory and Applications, 2(1), pp. 37-50. Available at: https://doi.org/10.31181/oresta1901015e.

Erstad, E. et al. 2023. CERP: A Maritime Cyber Risk Decision Making Tool. TransNav, International Journal on Marine Navigation and Safety of Sea Transportation, 17(2), pp. 269-279. Available at: https://doi.org/10.12716/1001.17.02.02.

Fazlollahtabar, H. et al. 2019. FUCOM Method in Group Decision-Making: Selection of Forklift in a Warehouse. Decision Making: Applications in Management and Engineering, 2(1), pp. 49-65. Available at: https://doi.org/10.31181/dmame1901065f.

Furumoto, K. et al. 2020. Toward Automated Smart Ships: Designing Effective Cyber Risk Management. In 2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), Rhodes, Greece, pp. 100-105. Available at: https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00034.

FURUNO. 2018. Operator's Manual Electronic Chart Display and FMD-3200. Available at: https://www.furuno.it/docs/OPERATOR%20MANUALOME44730M_FMD3200_FMD33000.pdf

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

Harish, A. V. et al., 2024. BridgeInsight: An Asset Profiler for Penetration Testing In a Heterogeneous Maritime Bridge Environment. Maritime Technology and Research, 6(1), pp. 266818-266818. Available at: https://doi.org/10.33175/mtr.2024.266818.

Hemminghaus, C. et al., 2021. BRAT: A BRidge Attack Tool for Cyber Security Assessments of Maritime Systems. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 15. Available at: https://doi.org/10.12716/1001.15.01.02.

IEC 61162-1, 2016. Maritime Navigation and Radiocommunication Equipment and Systems – Digital Interfaces – Part 1: Single Talker and Multiple Listeners. Available at: https://webstore.iec.ch/preview/info_iec61162-1%7Bed5.0%7Den.pdf

IEC 61162-2, 1998. Maritime Navigation and Radiocommunication Equipment and Systems – Digital Interfaces – Part 2: Single Talker and Multiple Listeners, High-Speed Transmission. Available at: https://webstore.iec.ch/preview/info_iec61162-2%7Bed1.0%7Db.pdf

IEC 61162-450, 2018. Maritime Navigation and Radiocommunication Equipment and Systems – Digital Interfaces – Part 450: Multiple Talkers and Multiple Listeners – Ethernet Interconnection. Available at: https://webstore.iec.ch/preview/info_iec61162-450%7Bed2.0%7Den.pdf

IEC 61174, 2015. Maritime Navigation and Radiocommunication Equipment and Systems – Electronic Chart Display and Information System (ECDIS) – Operational and Performance Requirements, Methods of Testing and Required Test Results. Available at: https://webstore.iec.ch/preview/info_iec61174%7Bed4.0%7Den.pdf

IEC 62065, 2014. Maritime Navigation and Radiocommunication Equipment and Systems – Track Control Systems – Operational and Performance Requirements, Methods of Testing and Required Test Results. Available at: https://webstore.iec.ch/preview/info_iec62065%7Bed2.0%7Den.pdf

IEC 62288, 2021. Maritime Navigation and Radiocommunication Equipment and Systems – Presentation of Navigation-Related Information on Shipborne Navigational Displays – General Requirements, Methods of Testing and Required Test Results. Available at: https://webstore.iec.ch/preview/info_iec62288%7Bed3.0.CMV%7Den.pdf

IHO, 2012. Guidance on Updating the Electronic Navigational Chart. International Hydrographic Organization. Available at: https://iho.int/uploads/user/pubs/standards/s-52/S-52_App1_ed4.0.0_Apr12.pdf

IHO, 2017. Information on IHO Standards related to ENC and ECDIS – Version 1.1. International Hydrographic Organization. Available at: https://iho.int/mtg_docs/enc/PSC_Advice_IHO_V1.1.pdf.

IHO, 2019. Information on IHO Standards Related to ENC and ECDIS. International Hydrographic Organization. Available at: https://legacy.iho.int/mtg_docs/enc/PSC_Advice_IHO_Ed2.0_Final.pdf

IMO, 2006. Adoption of the Revised Performance Standards for Electronic Chart Display and Information Systems (ECDIS). International Maritime Organization, Resolution MSC.232(82)/24/Add.2. 5 December 2006. Available at: https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.232(82).pdf

IMO, 2017. ECDIS – Guidance for Good Practice. International Maritime Organization, MSC.1/Circ.1503/Rev.1. 16 June 2017. Available at: https://www.classnk.or.jp/hp/pdf/activities/statutory/ism/imo/msc1-circ1503-rev1.pdf, accessed on: 24.02.2023.

Kala, N. & Balakrishnan, M. 2019. Cyber Preparedness in Maritime Industry. International Journal of Scientific and Technical Advancements, 5(2), pp. 19-28.

Karahalios, H. 2020. Appraisal of a Ship's Cybersecurity Efficiency: The case of Piracy. Journal of Transportation Security, 13(3-4), pp. 179-201. Available at: https://doi.org/10.1007/s12198-020-00223-1.

Kavallieratos, G. & Katsikas, S. 2020. Managing Cyber Security Risks of the Cyber-Enabled Ship. Journal of Marine Science and Engineering, 8(10), p. 768. Available at: https://doi.org/10.3390/jmse8100768.

Kayalvizhi, S. et al., 2016. Evaluation on Aggregation Risk Rate for Defuzzification in Fuzzy Sets. IJRDO - Journal of Computer Science Engineering, 2(11), pp. 01-06. Available at: https://doi.org/10.53555/cse.v2i11.879.

Kayisoglu, G. et al., 2022. Evaluating SLIM-Based Human Error Probability for ECDIS Cybersecurity in Maritime. The Journal of Navigation, 75(6), pp. 1364-1388. Available at: https://doi.org/10.1017/S0373463322000534.

Kessler, G. C., 2019. Cybersecurity in the Maritime Domain. USCG Proceedings of the Marine Safety & Security Council, 76(1), p. 34. Available at: https://commons.erau.edu/publication/1318.

Matić, B. et al., 2019. A New Hybrid MCDM Model: Sustainable Supplier Selection in a Construction Company. Symmetry, 11(3), p. 353. Available at: https://doi.org/10.3390/sym11030353.

Melnyk, O. et al., 2023. Integral Approach to Vulnerability Assessment of Ship's Critical Equipment and Systems. Transactions on Maritime Science, 12(01), pp. 3-3. Available at: https://doi.org/10.7225/toms.v12.n01.002.

Merrett, H. C. et al., 2019. Comparison of STPA and Bow-Tie Method Outcomes in the Development and Testing of an Automated Water Quality Management System. In MATEC Web of Conferences, 273, p. 02008. EDP Sciences. Available at: https://doi.org/10.1051/matecconf/201927302008.

Mokhtari, K. et al., 2011. Application of a Generic Bow-Tie Based Risk Analysis Framework on Risk Management of Sea Ports and Offshore Terminals. Journal of Hazardous Materials 192(2): pp. 465–75. Available at: https://doi.org/10.1016/j.jhazmat.2011.05.035.

NIST, 2023. Cybersecurity. National Institute of Standards and Technology. Available at: https://csrc.nist.gov/glossary/term/cybersecurity?ref=securityscientist.net#:~:text=The%20process%20of%20protecting%20information,NIST%20Cybersecurity%20Framework%20Version%201.1

Noureddine, M. & Ristic, M. 2019. Route Planning for Hazardous Materials Transportation: Multicriteria Decision Making Approach. Decision Making: Applications in Management and Engineering, 2(1), pp. 66-85. Available at: https://doi.org/10.31181/dmame1901066n.

Pamucar, D. & Ecer, F., 2020. Prioritizing the Weights of the Evaluation Criteria under Fuzziness: The Fuzzy Full Consistency Method–FUCOM-F. Facta Universitatis, Series: Mechanical Engineering, 18(3), pp. 419-437.

Pamucar, D. et al., 2018. Multi-Criteria FUCOM-MAIRCA Model for the Evaluation of Level Crossings: Case Study in the Republic of Serbia. Operational Research in Engineering Sciences: Theory and Applications, 1(1), pp. 108-129. Available at: https://doi.org/10.31181/oresta190120101108p.

Pamucar, D. et al., 2020. A Fuzzy Full Consistency Method-Dombi-Bonferroni Model for Prioritizing Transportation Demand Management Measures. Applied Soft Computing, 87, p. 105952. Available at: https://doi.org/10.1016/j.asoc.2019.105952.

Park, C. et al., 2023. A BN Driven FMEA Approach to Assess Maritime Cybersecurity Risks. Ocean & Coastal Management, 235, p. 106480. Available at: https://doi.org/10.1016/j.ocecoaman.2023.106480.

Park, S. et al., 2021. Importance–Performance Analysis (IPA) of Cyber Security Management: Focused on ECDIS User Experience. Journal of the Korean Society of Marine Environment and Safety, 27(3), pp. 429–38. Available at: https://doi.org/10.7837/kosomes.2021.27.3.429.

Progoulakis, I. et al., 2023. Digitalization and Cyber Physical Security Aspects in Maritime Transportation and Port Infrastructure. In: Johansson, T.M. et al. (eds) Smart Ports and Robotic Systems. Studies in National Governance and Emerging Technologies. Palgrave Macmillan, Cham. Available at: https://doi.org/10.1007/978-3-031-25296-9_12.

Shang, W. et al., 2019. Information Security Risk Assessment Method For Ship Control System Based On Fuzzy Sets And Attack Trees. Security and Communication Networks, 2019, pp. 1-12. Available at: https://doi.org/10.1155/2019/3574675.

Soner O. et al., 2023. Cybersecurity Risk Assessment of VDR. Journal of Navigation, 76(1), pp. 20-37. Available at: https://doi.org/10.1017/S0373463322000595.

Stevens, T., 2016. Cyber Security and the Politics of Time. Cambridge University Press.

Svilicic, B. et al., 2019a. Shipboard ECDIS Cyber Security: Third-Party Component Threats. Pomorstvo, 33(2), pp. 176–80. Available at: https://doi.org/10.31217/p.33.2.7.

Svilicic, B. et al., 2019b. Maritime Cyber Risk Management: An Experimental Ship Assessment. The Journal of Navigation, 72(5), pp. 1108-1120. Available at: https://doi.org/10.1017/S0373463318001157.

Svilicic, B. et al., 2019c. A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. Journal of Marine Science and Engineering, 7(10). Available at: https://doi.org/10.3390/jmse7100364.

Svilicic, B. et al., 2019d. Assessing Ship Cyber Risks: A Framework and Case Study of ECDIS Security. WMU Journal of Maritime Affairs, 18(3), pp. 509–20. https://doi.org/10.1007/s13437-019-00183-x.

Svilicic, B. et al., 2019e. Raising Awareness on Cyber Security of ECDIS. TransNav, 13(1), pp. 231–36. Available at: https://doi.org/10.12716/1001.13.01.24.

Tam, K. & Jones, K., 2019. MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment. WMU Journal of Maritime Affairs, 18(1), pp. 129–63. Available at: https://doi.org/10.1007/s13437-019-00162-2.

Tran, K. et al., 2021. Marine Network Protocols and Security Risks. Journal of Cybersecurity and Privacy, 1(2), pp. 239–51. Available at: https://doi.org/10.3390/jcp1020013.

Weintrit, A., 2009. The Electronic Chart Display and Information System (ECDIS): An Operational Handbook. CRC Press. Taylor & Francis Group, Florida, USA. Available at: https://doi.org/10.1201/9781439847640.

Yoo, Y. & Park, H. S. 2021. Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans In Consideration Of Digitalized Ship. Journal of Marine Science and Engineering, 9(6), p. 565. Available at: https://doi.org/10.3390/jmse9060565.