Ocean and Coastal Management 235 (2023) 106480

Contents lists available at ScienceDirect

Ocean and Coastal Management

journal homepage: www.elsevier.com/locate/ocecoaman

A BN driven FMEA approach to assess maritime cybersecurity risks

Changki Park, Christos Kontovas, Zaili Yang, Chia-Hsun Chang *

Liverpool Logistics, Offshore and Marine Research Institute (LOOM), Liverpool John Moores University, UK

ARTICLE INFO

Keywords:
Cybersecurity
Maritime risk
FMEA
Bayesian network
Maritime security

ABSTRACT

Cybersecurity risks present a growing concern in the maritime industry, especially due to the fast development of digitalised technologies, also vis-à-vis autonomous shipping. Research on maritime cybersecurity is receiving increased attention. This paper aims to assess the cybersecurity risks in the maritime sector and improve safety at sea and in coastal areas. First, we identify all the concerned cyber threats in the sector based on literature review and expert opinion. A novel risk assessment framework of maritime cyber threats, which combines Failure Mode and Effects Analysis (FMEA) with a Rule-based Bayesian Network (RBN), is proposed and used to evaluate the risk levels of the identified threats and to better understand the threats that contribute the most to the overall maritime cybersecurity risk. The results can inform stakeholders about the most vulnerable parts in their cyber operations and stimulate the development of risk-based control measures. More specifically, the next step in managing cyber threats is to tackle the threats that are associated with unacceptable risk levels and identify cost-effective measures to manage them. To that extent, our findings provide a list of top threats – that is the areas where efforts should be focused on. As a result, this work can help the whole community to grow its resilience to cyber-attacks and improve the security of shipping operations.

1. Introduction

In recent years, the shipping industry has been much concerned about a modern security aspect, the so-called cybersecurity, due to such factors as the increased use of Information Technology (IT) systems, automation and digitisation. Software and hardware systems are used, for example, in onboard vessels to control various processes such as navigation, engine and power management, and damage control systems monitoring, causing concerns related to maritime cybersecurity.

Maritime cyberattacks have been reported since the early 2010s. Recent representative incidents include (a) the 2020 ransomware attack that has hit the servers of container shipping giant CMA CGM, leading to the company's main website and applications being temporarily inaccessible (CMACGM, 2020), (b) the sophisticated-cyberattack which affected the International Maritime Organisation's (IMO) IT systems including the public web site and its internal intranet systems (Kovacs, 2020), and (c) the damage of equipment and information of containers by a cyberattack in a South Africa container operation company in July 2021 (Shead, 2021).

Accidents that occurred due to failure of addressing cyberattacks have witnessed huge consequences in terms of human fatalities, loss of assets and reputation, economic damages, environmental-related consequences and so on. For example, Maersk is reported to have lost $200–300 million due to a cyberattack in 2017, whereas the COSCO terminal at the Port of Long Beach in 2018, the IMO and CMA CGM in 2020 have suffered cyberattacks with network broken down for multiple days.

To respond to the increasing concerns on maritime cybersecurity, the IMO and the Baltic and International Maritime Council (BIMCO) - one of the world's major shipping associations-have led the relevant discussions at an international level, which resulted in the publication of the first-ever maritime cybersecurity guidelines (BIMCO, 2016).

In 2017, the IMO adopted its first guidelines on 'Maritime Cyber Risk Management' (IMO, 2017a), which were essentially based on the industry-led work published by BIMCO (BIMCO, 2016). Meanwhile, the IMO (2017b) adopted a resolution that *"encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the International Safety Management (ISM) Code) no later than the first annual verification of the company's Document of Compliance (DOC) after January 1, 2021"*. Note that the ISM code provides an international standard for the safe management and operation of ships at sea. Since 2021, shipowners and operators had to comply and address cyber risks in their existing safety management systems.

* Corresponding author.
E-mail addresses: c.park@2019.ljmu.ac.uk (C. Park), c.kontovas@ljmu.ac.uk (C. Kontovas), z.yang@ljmu.ac.uk (Z. Yang), c.chang@ljmu.ac.uk (C.-H. Chang).

https://doi.org/10.1016/j.ocecoaman.2023.106480
Received 27 June 2022; Received in revised form 21 November 2022; Accepted 3 January 2023
Available online 22 January 2023

Around the same time, leading classification societies and maritime authorities have formulated cyber-risk related guidelines. For example, DNVGL (2016) presented guidance (i.e., recommended practices) for ships and mobile offshore operations to improve their cybersecurity resilience management. Amongst others, it proposed an approach based on a Bow-Tie method to analyse the robustness of barriers against threats. The American Bureau of Shipping (ABS, 2016) has published 'Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations', a document that provides the practices for cybersecurity for both the marine and offshore industries. In addition to the documents published by classification societies, a number of maritime administrators have revealed issues on how shipowners could comply with the regulations (both national and international).

Risk assessment has been traditionally used to manage safety; in the aftermath of the 9/11 attacks shipping has become a target of what Lu et al. (2022) refer to as 'non-traditional safety events', which include piracy attacks and terrorism. However, the increasing reliance on IT leads to new challenges e.g., the introduction of cyber-related risks in shipboard operations (Karim, 2020). Digitalisation is also one of the main priorities of some ports (see for example Campisi et al., 2022) as they are using automation and innovative technologies to improve their performance. There is thus, now, the need to shift the focus from traditional safety and security towards cyber risks. Cyber risks need to be addressed in a proactive and systematic way – hence the need for risk assessment. In order to facilitate research on maritime cybersecurity, this paper aims to fill the current research gap by identifying maritime cyber threats, evaluating their risk levels and proposing countermeasures to improve maritime cybersecurity.

Several traditional risk assessment methods have been utilised in the maritime sector such as Hazard and Operability Studies (HAZOP), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Failure Mode and Effects Analysis (FMEA) (Wan et al., 2019a; Fan et al., 2020). Although there is an increasing number of maritime cybersecurity studies and maritime cybersecurity guidelines have been already published by international organisations, research addressing maritime cybersecurity risk assessment is still scant and often industry-driven from a practical perspective, in any case, falls behind compared to other industries (Caponi and Belmont, 2015), such as aviation (Suciu et al., 2019), autonomous vehicles (Khan et al., 2022), and healthcare (Coventry and Branley, 2018). The current maritime cybersecurity risk assessment is conducted using either qualitative analysis or very traditional quantitative risk analysis methods such using Bow-Tie analysis (Progoulakis et al., 2021) and risk matrices (Yoo and Park, 2021). However, security risks in general, and cybersecurity risks, in particular, suffer from high uncertainty in data. This sometimes makes the use of traditional risk approaches questionable, and the obtained risk estimation results arguable. There is, therefore, a significant research gap on how to incorporate advanced uncertainty modelling into improved maritime cybersecurity risk quantification and estimation, as further demonstrated in detail in Section 2.1.

This paper aims to use the combination of FMEA and Rule-based Bayesian Network (RBN) to estimate and prioritise the risk levels of maritime cybersecurity threats. FMEA and RBN have several advantages in dealing with high uncertainty in risk data and, therefore, have attracted increasing interest within risk assessment involving high uncertainty in data in recent years and used in various maritime-related research related to, for example, maritime supply chains (Wan et al., 2019a), autonomous ships (Chang et al., 2021), and container shipping services (Zhou et al., 2022). Its advance in tackling risk data fits well with maritime cybersecurity risk assessment given the very limited historical data available due to the limited number of accidents that occurred in the past. It is because of the high uncertainty in cybersecurity-related risk data that there are few studies on maritime cybersecurity risk analysis and fewer related to the use of advanced quantitative models for quantitative risk analysis of maritime cybersecurity. To the best of our knowledge, this is the first attempt to use a combined FMEA and RBN approach to address maritime cybersecurity risks. This paper will therefore make new contributions, a theoretical one which is presenting a novel cybersecurity risk analysis methodology based on RBN-FMEA and a practical one, the ranking of cybersecurity threats in maritime operations.

The rest of this paper is structured as follows. Section 2 presents a literature review with regards to the state of the art of maritime cybersecurity studies and the identification of cyber threats in the maritime industry, while section 3 describes the methodology to be used, in which the justification of the used FMEA-RBN method is presented. Section 4 describes and analyses the results of data analysis. Section 5 discusses the results and highlights the finding implications, and conclusions are drawn in Section 6.

2. Literature review

2.1. Cybersecurity: a bibliometric analysis and the research gap

In order to identify the important academic literature and to get useful insights of the literature, a bibliometric analysis has been, first, conducted.

The SCOPUS database has been used to identify documents related to cybersecurity in the maritime/shipping domain; the string *"(cybersecurity OR (cyber AND security)) AND (maritime OR shipping))"* has been used to search the title, abstract and keywords of the indexed documents. 314 have been identified and after a careful analysis of the documents we arrived at a dataset of n = 159 documents, of which half of them (i.e., 75 documents) are journal papers and the rest papers published in conference proceedings.

Looking at the annual scientific production, that is the number of papers published per year, there has been an increased engagement with the topic after 2016; with 21 documents published in 2018, 23 in 2019, 34 in 2020, 39 in 2021 and 19 until the first half of 2022. The relevant papers have been authored by 425 authors (an average of 3.4 co-authors), and most are co-authored works (with only 19 papers being single-authored ones). The earliest paper has been published in 2006; the scientific production has been very intensive in the last 4 years highlighting the growing importance and relevance of our work.

Content-wise, the first observation is that there is much computer security related literature, which is out of the scope of this work to describe. Then, there is literature related to risk management (and parts of the process such as risk identification, analysis and assessment) from a qualitative viewpoint. There are very few studies in the literature focusing on quantitative security risk analysis. If the security assessment cannot be assessed quantitatively, the established security management system does not motivate industrial professionals for its implementation, possibly because their effects are not visible in a state-of-the-art risk assessment (Yang et al., 2018). Within this context, Hossain et al. (2019) developed a Bayesian network for assessing and quantifying the resilience of a deep-water service port. Tam and Jones (2019) presented a framework for maritime cyber-risk assessment; whereas Svilicic et al. (2019) presented a risk analysis to identify and categorise cyber threats to ships. Bolbot et al. (2020) presented an interesting cyber-risk assessment method and as a case study, they apply their method for the cyber-risk assessment and design enhancement of the navigation and propulsion systems of an inland waterway autonomous vessel. A clear connection between cybersecurity and autonomous shipping has indeed been identified in the literature; see Chang et al. (2021).

Based on the above there is a clear need to deal with this increasingly important topic; both to comply with the relevant regulations and to protect systems against attacks that have proven to have significant consequences. At the same time, the literature on the topic is very scant and there is clear appetite for more research on the topic. The bibliometric analysis and the literature review have identified risk assessment as an important approach to manage the relevant risks.

Given this importance and the limited number of published works,

this paper will add significantly to the existing literature by performing a novel risk analysis and identifying the high-risk areas. This is an essential step as future research could use these findings and identify/develop rational measures to control the risk and evaluate their effectiveness.

2.2. Identification of maritime cyber threats

As discussed above due to the importance of the topic, companies must address and manage the related cybersecurity risks. Measures to control the risks should be sought with urgency. Before doing so though, the relevant threats need to be identified and consequently efforts should be focused on the most important ones; the latter could be achieved by prioritising the threats.

As the first step of risk analysis, one should start with the identification of significant cyber threats in the maritime domain. Indeed, many cyberattack accidents have been reported involving common cyber threats such as phishing, malware, ransomware, DDoS (Distributed Denial of Service), and man-in-the-middle attack (Ren et al., 2017; Lezzi et al., 2018). Through a literature review, six dimensions to categorise the maritime cyber threats are identified, including 'Phishing', 'Malware', 'Man in the middle attack', 'Thief of credentials', 'Human factor', and 'Using outdated IT systems'; see Table 1 for the threats discussed in the relevant literature. The detailed information of the threats is provided in the following sections.

2.2.1. Phishing

Phishing refers to sending a seeming impersonation email with links to fake websites, downloading malicious files (Qbeitah and Aldwairi, 2018) or text (Yeboah-Boateng and Amanor, 2014). The email may show that it is from a bank or other various legitimate businesses. Once the user clicks the links, all the information the user inputs to the fake website will be transferred to the hacker. These emails can be very deceiving and even an experienced user can be cheated. Sea crews using personal devices (e.g., smartphone, tablet, private USB device) could cause cybersecurity issues by receiving phishing emails or visiting malicious websites, and thus installing malicious viruses into vessel operational systems (BIMCO, 2018; Meland et al., 2021; Ben Farah et al., 2022).

2.2.2. Malware

Malware is malicious software that assesses or damages devices without the knowledge of the user, and further spreads the virus by downloading files attached to infected emails or accessing a fake website, or connecting USB drives and removable media containing malicious malware (Pham et al., 2010). It could lead to ransomware attacks or even Distribute Denial of Service (DDoS) (Jones et al., 2016; Ben Farah et al., 2022). In the maritime sector, IMO (2017a) and BIMCO (2018) have also listed malware as a severe threat to maritime cybersecurity given that malware could access and damage the operation systems of vessels or steal sensitive data from shipping companies. Meland et al. (2021) have listed a number of maritime cyberattacks caused by malware between 2010 and 2020. Mraković and Vojinović (2019) stated that malware is one of the major types of cyberattack in the maritime industry, and Alcaide and Llave (2020) argued that malware is the key choice of threat to carry out malicious intent to breach maritime cybersecurity.

2.2.3. Man in the middle attack

Through man in the middle attacks, hackers can obtain all the communication between different parties and/or pretend to be these parties. Hackers hide their presence in free/open WiFi hotspots or fake websites and prevent users from sending and receiving data or even redirect the information to another user (Mallik, 2019; Suciu et al., 2019). In the maritime industry, such cyber threat commonly attacks remote desktop protocol (RDP) services running on the Electronic Chart Display and Information System (ECDIS) (Svilicic et al., 2019).

2.2.4. Theft of credentials

Theft of credentials is a type of cyber threat that steals the proof of identity from users or customers. Insecure login systems and simple passwords can be easily targeted by hackers (Imran and Nizami, 2011). Boyes and Isbell (2017) proposed that some threat actor groups may break into servers or websites to steal users' credentials. A survey conducted by IHS Markit and BIMCO showed that 65 responders of the total 300 stakeholders in the maritime sector have experienced cyber threats, and 25% of them answered that they have been attacked by theft of credentials (Markit, 2016). According to the 2018 IHS Markit's survey, theft of credentials significantly increased from 2% in 2017 to 28% in 2018 (Markit, 2018).

2.2.5. Human factor

For shipping safety and security incidents, human factor has been recognised as a critical factor that directly and indirectly causes around 80–90% of accidents (Heij and Knapp, 2018; Chang et al., 2021). From a cybersecurity perspective, stakeholders who lack knowledge of

Table 1
List of reviewed papers and articles.

	Phishing	Malware	Man in the middle attack	Theft of credential	Human factor	Using outdated IT systems
Sen (2016)		✓				✓
Jones et al. (2016)		✓				✓
DNVGL (2016)		✓			✓	✓
IHS Markit (2016)	✓	✓		✓		
Tam and Jones et al. (2016)	✓	✓			✓	✓
IMO (2017a)		✓				
Boyes and Isbell (2017)		✓		✓	✓	
BIMCO (2018)	✓	✓			✓	✓
IHS Markit (2018)	✓	✓	✓	✓		
Park et al. (2019)	✓	✓			✓	✓
Mraković and Vojinović (2019)	✓	✓	✓	✓		
Svilicic et al. (2019)		✓	✓			✓
Alcaide and Llave (2020)	✓	✓			✓	
Androjna et al. (2020)		✓			✓	
Bolbot et al. (2020)	✓	✓	✓		✓	✓
Karahalios (2020)		✓			✓	
Meland et al. (2021)	✓	✓				
Senarak (2021)	✓	✓		✓	✓	✓
Ben Farah et al. (2022)	✓	✓	✓			✓
Khan et al. (2022)		✓			✓	
Tusher et al. (2022)	✓			✓	✓	✓

cybersecurity systems and do not follow cybersecurity processes make systems vulnerable to cyber accidents (Boyce et al., 2011). On the other hand, there are also insider threats, which means someone from within the organisation could harm them for individual benefits or specific purposes, such as stealing important data (Mazzarolo and Jurcut, 2019). Human factors are indeed seen as a main threat to maritime cybersecurity (Park et al., 2019; Senarak, 2021; Tusher et al., 2022). Hopcraft and Martin (2018) argued that the advancement of maritime industry technology has caused more ways for the maritime industry to expose cyber threats due to unintentional human error.

2.2.6. Using outdated IT systems

Sen (2016), Jones et al. (2016) and BIMCO (2018) analysed the vulnerability of maritime cybersecurity and found that shipping companies were over-reliant on outdated technology and were using outdated version of antivirus software, which are major threats. For example, some staff still believe that antivirus software and firewalls can fully protect the systems from cyberattacks. Without an up-to-date IT system, hackers can attack vessels or companies through viruses or malware, which is difficult to be detected and defended by traditional antivirus software (Sen, 2016; Park et al., 2019; Ben Farah et al., 2022; Tusher et al., 2022). Besides, many current ships were built way before the industry started considering cybersecurity as a major issue. Therefore, some ships and shipping companies are still using outdated IT and OT systems that are prone to cyberattacks.

3. Methodology

A hybrid method of FMEA with a RBN is employed to investigate the risk levels of the identified maritime cyber categories and threats in detail. Several traditional risk assessment methods have been utilised in the maritime sector such as the use of Delphi and risk matrices (Chang et al., 2015; Wan et al., 2019b), Hazard and Operability Studies (HAZOP), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), FMEA (Wan et al., 2019a; Fan et al., 2020); more recent approaches focus also on risk-based resilience (Wan et al., 2022). Considering not all cyber threats are detected and reported, this paper applies the concept of FMEA with three parameters (i.e., likelihood of failure, consequence of failure and probability of the failure being undetected) as the initial step of maritime cyber risk assessment. However, traditional risk assessment methods are not able to deal with the high uncertainty risk data in maritime cybersecurity; a more advanced technique should therefore be employed. The newly proposed FMEA-RBN methodology has revealed several advantages within the context of maritime cybersecurity. A key advantage of the model is its ability to incorporate both objective and subjective data; this is important when historical data is often unavailable or not reliable given the small number of the occurred accidents. The use of subjective data obtained through expert judgement also ensures that the results reflect the stakeholders experience and best practices. The inference process involving BN can inherently overcome one of the weaknesses of traditional FMEA which is the assumption that all three FMEA-parameters contribute equally towards the risk factor of an event (Hassan et al., 2022). In addition, the methodology can account for the difference in the experience and expertise of the experts; this could be done by setting different weights. RBN has been selected to build up the risk model in this paper due to its advantages such as modelling uncertain and complex domains (Uusitalo, 2007; Khan et al., 2021; Chen et al., 2022). Although there are a few attempts on using RBN in the maritime industry, to the best of our knowledge, this is the first attempt to use a combined FMEA and RBN approach to address maritime cybersecurity risks. The main novelties in terms of risk modelling are a) new definitions and descriptions of the three cybersecurity risk parameters and the linguistic terms used to define each of them and b) new conditional probability distribution to model the conditional relationship between the risk parameters and cybersecurity levels. In addition, with the validation through a sensitivity analysis, RBN provides a more reliable model and results. The details of FMEA and RBN are discussed in the following sections.

3.1. Failure modes and Effects Analysis (FMEA)

FMEA is a common method for investigating the importance of potential failure modes and is widely used for safety and reliability analysis in products and processes (Yang et al., 2008; Wan et al., 2019a). FMEA refers to risk in terms of severity, likelihood of failure mode/cause and detection; as per the IEC 60812:2018 standard. We should note here that FMEA has been used to address cybersecurity threats. For example, Asllani et al. (2018) proposed a so-called 'cybersecurity FMEA (C-FMEA) process' and reviewed the relevant literature; Haseeb et al. (2021) analysed cybersecurity in an Internet of Things environment; Kennedy et al. (2021) addressed human factors and cybersecurity in the context of Australian rail industry using FMEA. For consistency, we keep the traditional FMEA terminology and hereafter any reference to 'failures' or 'failure modes' denotes threats.

Risk Priority Number (RPN), denoted by S, is the main component of FMEA and derived by combining assessments made on ordinal scales with values for likelihood (L), detectability (P) and consequence (C) as follows:

$$S = L \times C \times P$$

When lacking historical failure data, the three parameters are often defined by linguistic terms in order to better describe and model subjective assessments (Yang et al., 2008; Alyami et al., 2019). The Likelihood of threats (L) is determined using five linguistic terms (*Li, i = 1,2, …, 5*): very low, low, average, high, and very high. Consequence (C) is estimated by five terms (*Ci, i = 1,2, …, 5* $\mathrm{Ci,i} = 1,2,\ldots,5$): negligible, marginal, moderate, critical, and catastrophic. The Probability of the failure being undetected (P) is determined using the following five terms (*Pi, i = 1,2, …, 5* $\mathrm{Pi,i} = 1,2,\ldots,5$): highly unlikely, unlikely, average, likely, and highly likely. The definitions of the five levels for these three parameters are shown in Tables 2–4. Finally, the RPN for each threat is defined using five linguistic terms (*Si, i = 1,2, …, 5*): very low, low, average, high, and very high.

3.2. FMEA rule-based bayesian networks (FMEA-RBN)

We adapt the approach proposed by Yang et al. (2008) and apply it within the new maritime cybersecurity context by defing the following six steps.

(1) Identify the threats in maritime cybersecurity
(2) Develop the Bayesian network
(3) Establish rule-based systems with degree of belief (DoB) in FMEA-RBN
(4) Aggregate rules with a Bayesian Reasoning mechanism
(5) Convert the results into crisp values with utility functions
(6) Validate using sensitivity analysis

Step 1: Identify threats in maritime cybersecurity

Table 2
The definition of likelihood for maritime cybersecurity.

Likelihood of maritime cyberthreat	Definition
Very Low (VL)	The cyberthreat is rare but might happen during lifetime
Low (L)	The likelihood of the threat is around once a year
Average (A)	The likelihood of the threat is occasional (e.g., once a quarter)
High (H)	The likelihood of the threat is repeated (e.g., once a month)
Very High (H)	The likelihood of the threat is almost certain

Source: adapted from Alyami et al. (2019) et al. and Chang et al. (2021).

Table 3
The definition of consequence for maritime cybersecurity.

Consequence of maritime cyberthreat	Definition
Negligible (N)	The consequence of the threat is limited. It only requires a minor maintenance.
Marginal (MA)	The threat causes a marginal system damage. The system operations are slightly interrupted. It requires a short period (e.g., less than 6 h) to fix the system.
Moderate (MO)	The threat causes a moderate system damage. The system operations are interrupted. It requires a longer period (e.g., more than 12 h) to fix the system.
Critical (CR)	The threat causes a major system damage. The system operations need to be stopped. High degree of operational interruption occurs.
Catastrophic (CA)	The threat causes a total system loss. Extremely serious consequence that affects sailing operations occurs.

Source: adapted from Alyami et al. (2019) et al. and Chang et al. (2021).

Table 4
The definition of probability of the threat being undetected for maritime cybersecurity.

Probability of the failure being undetected	Definition
Highly unlikely (HU)	The threat could be detected without checks or maintenance
Unlikely (U)	The threat could be detected by regular checks or maintenance
Average (A)	The threat could be detected by intensive checks or maintenance
Likely (L)	The threat is difficult to be detected by intensive checks or maintenance
Highly likely (HL)	The threat is impossible to be detected even by intensive checks or maintenance

Source: adapted from Alyami et al. (2019) et al. and Chang et al. (2021).

Based on the literature review and the results of Questionnaire 1, six maritime cyber threat categories are identified, including 'Phishing', 'Malware', 'Man-in-the-middle attack', 'Theft of credential', 'Human factor', and 'Using outdated IT systems'. Each threat category consists of several threats.

Step 2: Develop the Bayesian network

After the identification, the threat categories and threats are further used to build up a BN model. Fig. 1 illustrates the developed BN model to be used in this study; threats are illustrated with yellow ovals (root nodes) and threat categories are represented with orange ovals (leaf nodes).

Step 3: Establish rule-based systems with a DoB in FMEA-RBN

A rule-based approach is applied to define the causation relationships and impact levels among the nodes of the BN. It uses several rules to describe the relationship between the *IF* and *THEN* parts, which are used to convert p attendance attributes $\{A_1, A_2, \ldots, A_p\}$ (*IF* part) into q states $\{C_1, C_2, \ldots, C_q\}$ (*THEN* part) by assigning a belief degree β_s ($s = 1, 2, \ldots, q$) to Cs ($s \in q$) $\in$q). For example, the *w*th *IF-THEN* rule (denoted as R_w) in a rule-based set can be expressed as:

$$R_w: \textbf{IF } A_1^w \text{ and } A_2^w \text{ and } \ldots \text{ and } A_p^w, \textbf{THEN } \left\{\left(\beta_{1,}^w C_1\right), \left(\beta_{2,}^w C_2\right), \ldots, \left(\beta_{q,}^w C_q\right)\right\}.$$

The *IF* part is a set of linguistic states $A^w = \{A_1^w, A_2^w, \ldots, A_p^w\}$ in a R_w, and a set of DoB in the *THEN* part can be expressed as $\{(\beta_{1,}^w C_1), (\beta_{2,}^w C_2), \ldots, (\beta_q^w, C_q)\}$ for the description of how each C_s ($s = 1, 2, \ldots, q$) is believed to be the result of β_s R_w, which can be assigned with experience or by using converting methods e.g., the equivalent influential method presented in Yang et al. (2008). After combining all rules, we can then develop a rule-based structure with multiple inputs and outputs.

When conducting the IF-THEN rules, this research applies a belief structure that helps identify the respondents' knowledge of the specific threats. The rules with belief structures in FMEA can be established based on expert judgment. Table 5 shows a three-parameters DoB distribution for the 125 rules (5^3).

As per the above-mentioned approach, several rules are used in the FMEA-RBN maritime cybersecurity model. For example, an IF-THEN rule to describe the relationship among the three parameters in the FMEA-RBN is defined as follows.

R_1: IF very low (L1), negligible (C1), and very unlikely (P1),

THEN S is {(1, very low risk (S1)), (0, low risk (S2)), (0, average (S3)), (0, high risk (S4)), (0, very high risk (S5))}.

R_2: IF very low (L1), negligible (C1), and unlikely (P2),

THEN S is {(0.67, very low (S1)), (0.33, low (S2)), (0, average (S3)), (0, high (S4)), (0, very high (S5))}.

The explanation of the above rule is as follows.

R_1: if the likelihood of the threat is very low, the consequence is negligible, and the probability of the failure being undetected is very unlikely, then the risk level of the threat is very low with a 100% DoB, low with a 0% DoB, average with a 0% DoB, high with a 0% DoB, and very high with a 0% DoB.

R_2: if the likelihood of the threat is very low, the consequence is negligible, and the probability of the failure being undetected is unlikely, then the risk level of the threat is very low with a 67% DoB, low with a 33% DoB, average with a 0% DoB, high with a 0% DoB, and very high with a 0% DoB.

Step 4: Aggregate rules through a Bayesian Reasoning mechanism

The observation information (e.g., obtained through expert judgement) are aggregated by using the Bayesian Reasoning mechanism, in

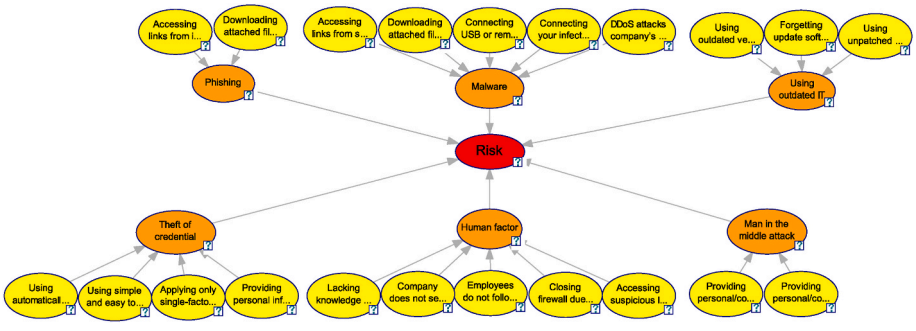

Fig. 1. The maritime cybersecurity BN model.

Table 5
The established RBN with a belief structure.

Rule	Parameters in the IF part			DoB in the THEN part				
No	L	C	P	S1	S2	S3	S4	S5
1	Very low (L1)	Negligible (C1)	Very unlikely (P1)	1				
2	Very low (L1)	Negligible (C1)	Unlikely (P2)	0.67	0.33			
3	Very low (L1)	Negligible (C1)	Average (P3)	0.67		0.33		
4	Very low (L1)	Negligible (C1)	Likely (P4)	0.67			0.33	
5	Very low (L1)	Negligible (C1)	Very likely (P5)	0.67				0.33
…	…	…	…	…	…	…	…	…
121	Very high (L5)	Catastrophic (C5)	Very unlikely (P1)	0.33				0.67
122	Very high (L5)	Catastrophic (C5)	Unlikely (P2)		0.33			0.67
123	Very high (L5)	Catastrophic (C5)	Average (P3)			0.33		0.67
124	Very high (L5)	Catastrophic (C5)	Likely (P4)				0.33	0.67
125	Very high (L5)	Catastrophic (C5)	Very likely (P5)					1

which a BN is developed for information aggregation. In the BN, a graphical network, firstly, describes the relationships of root nodes to the leaf node. A conditional probability table (CPT) for each node is, then, developed by converting the IF-THEN rules (i.e. DoB in the THEN part of each rule) into a CPT. Table 6 presents the CPT for the risks used in the FMEA-RBN methodology.

In Table 6, the first rule of the threat level (yellow level in Fig. 1) can be expressed as follows:

R_1: IF L1, C1 and P1, THEN {(1, (S1)), (0, (S2)), (0, (S3)), (0, (S4)), (0, (S5))}

This represents a condition where given L1 and C1 and P1, the probability of S (DoB) is p (R|L1, C1, P1) = (1, 0, 0, 0, 0).

For the category level (orange level in Fig. 2), there are different numbers of threats under each category. For example, 'Phishing' and 'Man in the middle attack' have 2 threats (5^2 = 25 rules), 'Using outdated IT system' has 3 threats (5^3 = 125 rules), 'Theft of credential' has 4 threats (5^4 = 625 rules), and 'Human factor' and 'Malware' have 5 threats (5^5 = 3125 rules). To save space, we present a selected (i.e., 5th) rule of 'Phishing' as follows.

R_5: IF Phishing threat 1 is very high, and Phishing threat 2 is very low, THEN the risk of 'Phishing' is {(0.5, (S1)), (0, (S2)), (0, (S3)), (0, (S4)), (0.5, (S5))}.

In terms of overall risk (red level in Fig. 2), this has 6 threat categories (5^6 = 15,625 rules), and for example, the 195th rule for the overall risk can be expressed as follows.

R_{195}: IF 'Phishing' is very high, 'Malware' is very high, 'Man in the middle attack' is high, 'Theft of credential' is average, 'Human factor' is low, and 'Using outdated IT systems' is very low, THEN the overall risk is {(0.33, (S1)), (0.17, (S2)), (0.17, (S3)), (0.17, (S4)), (0.17, (S5))}. From the above illustrative examples, it can be seen that the DoB assigned in the THEN part are based on the proportion distribution with the condition of each element in the IF part carrying the same weight.

Once the model is developed, the prior probabilities, which is the observed information, will be aggregated to calculate the marginal probabilities. After analysing the prior probabilities of all nodes, the marginal probability p (R_h) for the result can be calculated as follows (Yang et al., 2008):

$$p(R_h) = \sum_{i=1}^{5}\sum_{j=1}^{5}\sum_{k=1}^{5} p\left(R\middle|L_i, C_j, P_k\right)p(L_i)p\left(C_j\right)p(P_k), (h = 1, \ldots, 4)$$

Step 5: Convert the results into crisp values with utility functions

A set of utility values are assigned to the target node 'Risk' in the FMEA-RBN model to illustrate the importance of threats from different scenarios. In this paper, they are combined to prioritise the threats and threat categories. For example, from low-risk influence to high-risk influence, the utility values assigned to L, C and P are $U_{L1} = U_{C1} = U_{P1} = 1$; $U_{L2} = U_{C2} = U_{P2} = 2$, $U_{L3} = U_{C3} = U_{P3} = 3$, $U_{L4} = U_{C4} = U_{P4} = 4$ and $U_{L5} = U_{C5} = U_{P5} = 5$ (Chang et al., 2021). On this basis, five IF-THEN rules (see Table 5) are used to combine the utility values for R, including Rule 1, Rule 32, Rule 63, Rule 94 and Rule 125, in which.

R1: IF L1, C1 and P1, THEN {(1, (R1)), (0, (R2)), (0, (R3)), (0, (R4)), (0, (R5))};
R32: IF L2, C2 and P2, THEN {(0, (R1)), (1, (R2)), (0, (R3)), (0, (R4)), (0, (R5))};
R63: IF L3, C3 and P3, THEN {(0, (R1)), (0, (R2)), (1, (R3)), (0, (R4)), (0, (R5))};
R94: IF L4, C4 and P4, THEN {(0, (R1)), (0, (R2)), (0, (R3)), (1, (R4)), (0, (R5))};
R125: IF L5, C5 and P5, THEN {(0, (R1)), (0, (R2)), (0, (R3)), (0, (R4)), (1, (R5))}.

Therefore,

$U_{R1} = U_{L1} * U_{C1} * U_{P1} = 1$

$U_{R2} = U_{L2} * U_{C2} * U_{P2} = 8$

Table 6
The CPT for the FMEA-RBN.

L	L1							L5					
C	C1				C5			C1				C5	
P	P1		P5		P1	…	P5	P1		P5		P1	…	P5
S1	1	…	0.67	…	0.67		0.33	…	0.67	…	0.33	…	0.33		0
S2	0		0		0		0		0		0		0		0
S3	0		0		0		0		0		0		0		0
S4	0		0		0		0		0		0		0		0
S5	0		0.33		0.33		0.67		0.33		0.67		0.67		1

$U_{R3} = U_{L3}*U_{C3}*U_{P3} = 27$

$U_{R4} = U_{L4}*U_{C4}*U_{P4} = 64$

$U_{R5} = U_{L5}*U_{C5}*U_{P5} = 125$

The crisp values (CV) are calculated by using the utility function below:

$$CV = \sum_{z=1}^{t} p(R_h) U_{Rz}$$

where t is the number of linguistic terms of a node, p (R_h) the marginal probability and $U_R z$ (z = 1, 2, 3, 4, 5) the synthesised utility value assigned to R. Utility values can be then assigned to calculate the risk levels of all the threats and threat categories and express them into crisp values for a risk ranking purpose. The larger the value, the higher the associated security risk is.

Note that in this work a linear utility function is used in line with the literature, see for example Wan et al. (2019a), Yu et al. (2020) and Chang et al. (2021). At the same time, we assume equal importance for threats and threat categories. Weights could have been used to assign, for example, greater importance to the opinion of, say, specific experts or specific threats/categories. This would have required more evidence though as to why specific experts or different threats are more important

Table 7
The results of Questionnaire 1.

Threats Category	Risk level	Threats of Maritime Cybersecurity
Phishing	3.58	Accessing links from impersonation emails (e.g., bank, credit card company, insurance company, etc.)
	3.55	Downloading attached files from impersonation emails (e.g., bank, credit card company, insurance company, etc.)
	2.88	Accessing links from impersonation text messages (e.g., bank, credit card company, insurance company, etc.)
Malware	3.09	Downloading files (e.g., mp3, movie, games) from suspicious websites
	3.94	Accessing links from suspicious emails
	3.39	Downloading attached files from unknown emails
	4.03	Connecting USB or removable media to computer without virus check
	2.91	Accessing malicious advertising on websites
	3.82	Connecting your infected USB or removable media to connect computers/navigation systems
	3.58	DDoS attacks company's server system
Man-in-the-middle-attack	2.67	Using unsecured open Wi-Fi connections
	2.82	Using insecure Virtual Private Network (VPN)
	2.67	Applying weak WEP/WPA encryption on access points
	3.33	Providing personal/commercial information to friends/partners via open Wi-Fi connection
	3.36	Providing personal/commercial information to suspicious websites (e.g., illegal software/music/movie download websites)
Theft of credentials	3.48	Using automatically log in system (e.g., save your ID and password on websites)
	3.58	Using simple and easy to assume passwords
	3.33	Applying only single-factor authentication for login account system
	3.24	Providing personal information to a fake website (e.g., government website, etc.)
Human factor	4.15	Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it)
	3.70	Company does not set a proper cybersecurity process
	4.06	Employees do not follow company's cybersecurity process due to poor cybersecurity awareness
	3.76	Closing firewall due to careless operations or specific purpose
	3.55	Accessing suspicious links due to careless operations or specific purpose
Using outdated IT systems	3.70	Using outdated version firewall and antivirus software
	3.70	Using unpatched operating systems e.g., outdated window version
	3.27	Forgetting update software
	3.09	No planning applying up-to-date software

than others, a more complex questionnaire and potentially a more complex methodology e.g., the use of Evidential Reasoning (Yu et al., 2020).

Step 6: Model Validation

Sensitivity analysis refers to the sensitivity of the model performance to changes in parameters (Ren et al., 2008). It can help in checking whether the model is reliable. Sensitivity analysis is widely used in BN analysis and can be conducted in different ways, e.g., Yang et al. (2008) conducted sensitivity analysis by shifting the percentage of a linguistic level through Excel; whereas Yu et al. (2020) and Chang et al. (2021) focused on the changes in several certain linguistic levels using the GeNIe software. In this study, a sensitivity analysis is conducted to analyse how the identified cyber threats affect the entire risk through GeNIe. In addition, an added step of validation is conducted. If the model is robust, it should at least satisfy the following two axioms (Jones et al., 2010).

Axiom 1. An increase/decrease in the probabilities of each cyber threat should generate a relative increase/decrease to the risk.

Axiom 2. Given the variation of the probability distributions of each cyber threat, its influence magnitude on the risk values should keep consistency.

4. Data analysis

4.1. Results of the first run questionnaire

To analyse the risk level of the six identified maritime cyber threat categories and a list of threats, a new methodology is developed. The threats and the categories identified from the literature are first validated and initially evaluated by domain maritime experts to make sure that they are comprehensive and representative. A semi-structured questionnaire with a five-point Likert scale (Questionnaire 1) is distributed to experts who work in relevant stakeholders such as shipping companies, port operators and academia. In Appendix Awe present the structure of this questionnaire. Table A1 presents a sample of the threats that were rated; the full list of threats appears in Table 7. Questionnaire 1 is designed with a five-point Likert scale, from 1: very low risk to 5: very high risk, and includes the following three purposes: (1) to validate the identified threats, (2) to explore more threats not identified from the literature review, and (3) to screen the importance of the identified threats for a further more in-depth analysis (to be performed using Questionnaire 2).

In total, 100 copies of Questionnaire 1 were sent out to shipping companies, seafarers, port authorities, IMO experts, and academics. 38 replies have been received, of which 31 were complete (valid response rate: 31%) and have been used to prioritise the importance of the assessed threats.

Based on the experts' opinion, the top two threats are identified as 'Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it)' and 'Employees do not follow company's cybersecurity process due to poor cybersecurity awareness'; both belong to the 'Human factor' category. The third most concerned threat is 'Connecting USB or removable media to computer without virus check', which belongs to the 'Malware' category. The fourth and fifth also belong to this category and are 'Accessing links from suspicious emails' and 'Connecting your infected USB or removable media to connect computers/navigation systems', respectively.

The full results of Questionnaire 1 are presented in Table 7. The threats with relative importance (see threats highlighted in green) were

Table 8
Respondents' background.

Organisation	Shipping company	34
	Port operator	4
	Academia	6
Work experience	Less than 5 years	13
	6–10 years	11
	11–15 years	12
	More than 16 years	8

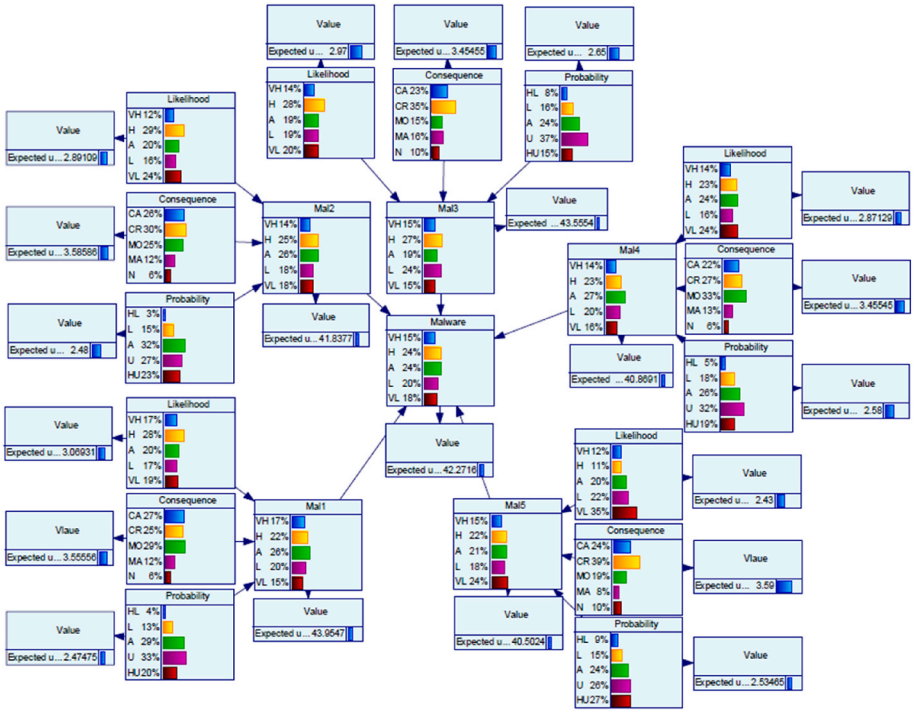

Fig. 2. Result of the assessment of the 'Malware' threat category.

Table 9
Risk values of threat categories and threats from Questionnaire 2.

Threat category	Category value	Threat	Threat value	Rank
Phishing	40.24	**Accessing links from impersonation emails (e.g., bank, credit card company, insurance company, etc.) (Ph1)**	**41.26**	**5**
		Downloading attached files from impersonation emails (e.g., bank, credit card company, insurance company, etc.) (Ph2)	39.22	9
Malware	42.27	**Accessing links from suspicious emails (Ma1)**	**43.95**	**1**
		Downloading attached files from unknown emails (Ma2)	**41.84**	**4**
		Connecting USB or removable media to a computer without virus check (Ma3)	**43.56**	**2**
		Connecting your infected USB or removable media to connect computers/ navigation systems (Ma4)	40.87	6
		DDoS attacks company's server system (Ma5)	40.5	8
Men-in-the-middle attack	35.31	Providing personal/commercial information to friends/partners via open Wi-Fi connection (MITM1)	35.68	15
		Providing personal/commercial information to suspicious websites (e.g., illegal software/music/movie download websites) (MITM2)	34.94	17
Theft of credential	37.27	Using automatically log in system (e.g., save your ID and password on website) (TC1)	38.34	10
		Using simple and easy to assume passwords (TC2)	37.56	11
		Applying only single-factor authentication for login account system (TC3)	34.79	18
		Providing personal information to a fake website (e.g., government website, etc.) (TC4)	37.2	12
Human factor	38.27	**Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it) (HE1)**	**41.95**	**3**
		Company does not set a proper cybersecurity process (HE2)	35.52	16
		Employees do not follow company's cybersecurity process due to poor cybersecurity awareness (HE3)	40.71	7
		Closing firewall due to careless operations or specific purpose (HE4)	35.87	14
		Accessing suspicious links due to careless operations or specific purpose (HE5)	36.65	13
Using outdated IT	29.12	Using outdated version firewall and antivirus software (IT1)	31.4	19
		Using unpatched operating system e.g., outdated window version (IT2)	28.93	20
		Forgetting update software (IT3)	27.15	21

Note: red colour refers to risk value more than 40; yellow colour refers to risk value between 30 and 40; green colour refers to risk value less than 30.

selected for a more thorough investigation through Questionnaire 2 and the application of our novel FMEA-RBN methodology.

4.2. Results of FMEA-BRN

Questionnaire 2 (see Appendix B) was used to collect the DoB of the three parameters: likelihood (L), consequence (C) and probability of failure of being undetected (P) of the selected threats identified through Questionnaire 1. The reason for using the DoB is that it considers respondents' uncertainty when answering questions.

In total, we have sent Questionnaire 2 to 100 maritime industry experts, who have rich experience in the maritime industry and are familiar with the topic of cyber-security. Respondents were asked to provide a percentage to each statement using five levels of linguistic terms; see Tables 2–4 for the definitions of the levels of each parameter against each selected threat in Table 7. These parameters were presented in a table format, see Table B1 (Appendix B). for a sample of the rating input table; the full list of threats presented to the experts is the one obtained by Questionnaire 1 and shown in Table 7.

For each parameter, the sum of the DoB of the five-level items should be 100%. For instance, a valid response would be that an expert believes that the likelihood of 'Accessing links from impersonation emails (e.g., bank, credit card company, insurance company, etc.)' is 30% High, and 70% Average, and the consequence is 40% Moderate and 60% Marginal, whereas for the probability of failure being undetected is 100% Likely. A total of 48 replies were collected, of which 44 replies were complete (valid response rate 44%). The respondents' background is summarised in Table 8; 77.27% of them work in a shipping company, followed by 9% in the port industry and 13.63% academic researchers in the maritime field. In addition, 46.46% of them have more than 10 years of experience.

The results show that the value of likelihood of Ma1 is around 3.06, with 17% of Very High (VH), 28% of High (H), 20% of Average (A), 17% of Low (L), and 19% of Very Low (VL). Whereas the value of consequence is around 3.56, with 27% of Catastrophic (CA), 25% of Critical (CR), 29% of Moderate (MO), 12% of Marginal (MA), and 6% of Negligible (N). The value of probability of the failure being undetected is around 2.47, with 4% of Highly likely (HL), 13% of Likely (L), 29% of

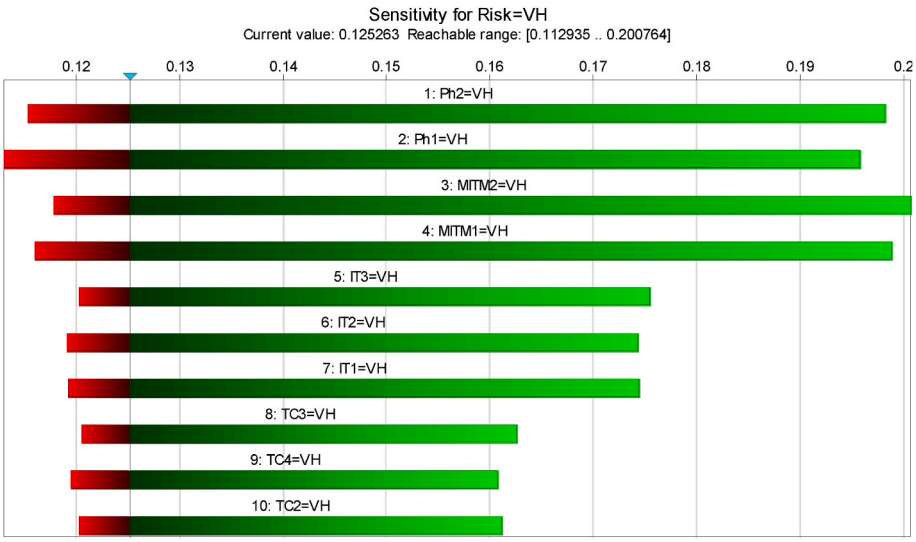

Fig. 3. Sensitivity analysis in very high overall risk.

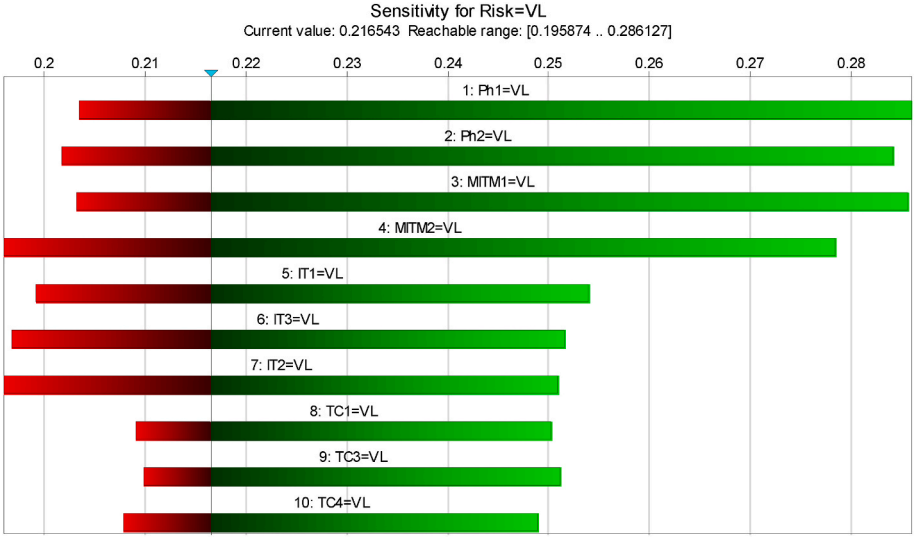

Fig. 4. Sensitivity analysis in very low overall risk.

Average (A), 33% of Unlikely (U), and 20% of Highly Unlikely (HU).

For example, our calculations, using the utility function, arrive at a value of 43.95 for 'Accessing links from suspicious emails (Ma1)'; the value of 'Downloading attached files from unknown emails (Ma2) is 41.84, for 'Connecting USB or removable media to a computer without virus check' (Ma3) is 43.56, for 'Connecting your infected USB or removable media to connect computers/navigation systems (Ma4)' is 40.87 etc.

For an illustrative purpose, we present the results of the 'Malware' threat category in Fig. 2 and we summarise the risk value of each threat category and threat related to maritime cybersecurity in Table 9. The results show that the threat category of 'Malware' has the highest risk value (risk value 42.27), followed by 'Phishing' (risk value: 40.24), and 'Human factor' (risk value: 38.27); whereas the least important threat category is that of 'Using outdated IT' (risk value: 29.12).

Overall, the top three threats include 'Accessing links from suspicious emails' (Ma1, risk value: 43.95), 'Connecting USB or removable media to a computer without virus check' (Ma3, risk value: 43.56), and 'Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it)' (risk value: 41.95); whereas the least three important threats that contribute to maritime cybersecurity risk are 'Forgetting to update software' (risk value: 27.15), 'Using unpatched operating system e.g., outdated window version' (risk value: 28.93), and 'Using outdated version firewall and antivirus software' (risk value: 31.4).

4.3. *Validation and sensitivity analysis*

The BN-based model requires validation to check whether the model is robust and to ensure the reliability of the results. An in-person meeting is also conducted to have a validation of the rationality of the proposed model with three experts from the maritime industry: (1) A captain with more than 20 years of work experience who has a number of experiences dealing with cyberattacks on board; (2) An IT manager of a container shipping company with more than 15 years of work experience; and (3) A maritime-related research scholar with more than 15 years of work experience. All experts agree with the rationale for the framework, as well as its elements and structure. Both questionnaires have also been validated by the three experts.

In order to carry out the full validation of the model, a comprehensive set of data related to cybersecurity incidents needs to be collected, which is impractical at this stage of the research. Due to lack of

comprehensive data, our validation is performed through a sensitivity analysis in line with Jones et al. (2010). Meanwhile, both questionnaires lead to similar results as it has been illustrated above, i.e., the top three threats identified from Questionnaire 2 are among the top five threats identified using Questionnaire 1. In addition, we have carried out a sensitivity analysis in line with similar studies, see for example Yang et al. (2008), Yu et al. (2020) and Chang et al. (2021). The used software implements a simple algorithm; given a set of target nodes, a complete set of derivatives of the posterior probability distributions over the target nodes (in our case, the overall risk) can be calculated. If the derivative is large for a parameter, a small change in it may lead to a large change in the posteriors of the targets. The bar shows the changes of the overall risk from the change of each threat.

The sensitivity analysis is to investigate the impact of various threats on the overall risk. Two extreme results are listed for illustration purposes: the overall risk being 'very high' (Fig. 3) and 'very low' (Fig. 4). In Fig. 3, the value of Ph2 varies between 0.1153 and 0.1983, implying the 'very high' of the overall risk will increase to 0.1983 when setting Ph2 to 100% 'very high' (keeping the other threats the same); whereas the 'very high' of the overall risk will decrease to 0.1153 when setting Ph2 to 0% 'very high'. Therefore, Ph2 has the highest impact on the overall risk among all threats. Meanwhile, TC2 (the last bar in Fig. 4) shows the lowest impact on the overall risk. In this process, the setting of Ph2 is changed from 0% 'very high' to 100% 'very high' with a step of 10%. The impact of every change to the target node 'risk' is consistently increased, which is in line with Axiom 1. In a similar way, the impact levels of the threats are also in good harmony with their importance. It proves the model against Axiom 2.

Fig. 3 illustrates that in the context of 'very high' (VH) overall risk, 'Accessing links from impersonation emails (e.g., bank, credit card company, insurance company, etc.) (Ph1)' and 'Downloading attached files from impersonation emails (e.g., bank, bank, credit card company, insurance company, etc.) (Ph2)' have the most significant impact on the overall risk. In contrast, the one with the lowest impact on the overall risk is using outdated IT systems (see the red part of the IT3), which indicates that forgetting to update software will result in a relatively low impact compared to the highly ranked threats.

Fig. 4 shows two critical situations influencing the overall risk of maritime cybersecurity: (a) 'Not providing personal/commercial information to suspicious websites as opposed to providing personal/commercial information to suspicious websites (e.g., illegal software/music/movie download websites)' would significantly decrease the overall risk to a 'very low' level (see the green part of MITM2) and (b) 'Accessing links from impersonation emails (e.g. bank, credit card company, insurance company, etc.)' will largely increase the overall risk (the red part of PH1). In addition, Fig. 4 also depicts that 'Providing personal information to fake websites' should not be considered in a very low overall maritime cybersecurity risk as it has limited positive impact (the green part of TC4).

Although not in the top five threats, as we can see in Figs. 3 and 4, Ph1, Ph2, MTM1, and MTM2 have revealed significant impact on the overall risk. By controlling these threats, we can significantly reduce the overall risk because of their high impact and sensitivity.

5. Discussions

The results in Section 4 show that 'Malware' is the most important cybersecurity risk category. This indicates that the maritime industry should try to identify some measures either to mitigate the impacts of the consequences of malware or to preventing them by reducing the likelihood or probability of the threat being undetected. However, the top values are just in the middle between U_{R3} (27) and U_{R4} (64), which indicates that most of the respondents feel that cyber threats do not significantly impact the maritime industry. On the other side, the lowest cyber threat category is 'Using outdated IT systems' with a value very close to U_{R3} (27), which refers to that the respondents do not think this is an important factor that contributes to the maritime cybersecurity risk. By checking the aggregated data, we found that the likelihood of the three cyber threats is the lowest among the three parameters, which implies that most of the respondents believe that their companies have updated the IT to the latest version to protest the damage from the cyberattacks.

There are eight threats that have values above 40; the top three threats are 'Accessing links from suspicious emails (Ma1)', 'Connecting USB or removable media to a computer without virus check (Ma3)', and 'Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it) (HE1)'. The top two cyber threats belong to the category of 'Malware', which has been identified as the top cyber-risk category and illustrates the importance of addressing this area. Sea crew and company staff might attempt to operate navigational or company's IT systems in convenient ways, which might cause more cyber vulnerability and a higher likelihood to be cyberattacked. However, these top three cyber threats can all be controlled through increased cybersecurity awareness, which could be gained through regular training and education.

5.1. Practical implications of the findings

This study presents a novel risk assessment of maritime cyber threats; it analyses the identified cyber threats, analyses their risks for their prioritisation. The next step in managing cyber threats is to focus on those threats that are associated with unacceptable risk and identify cost-effective measures to manage them. To that extent, the findings provide a list of top threats – that is the areas where efforts should be focused on. In light of this, some countermeasures that could address the top threats are put forward. It provides the foundation for the development of a new decision-making method to realise the risk-based optimal selection of cost-effective security measures.

1. Education, Training, and Awareness are key. Experts feel that 'Lacking knowledge of cybersecurity (i.e., facing a new situation and do not know how to deal with it) (HE1)' is one of the top threats. Training and education of people about the risks, particularly awareness improvement are essential. It is to impart fundamental knowledge and tools. Regular training will help attain awareness. Many studies have suggested that training and educating seafarers and staff is an effective method to improve maritime cybersecurity (Jones et al., 2016; Bolbot et al., 2020; Kanwal et al., 2022). They suggested that seafarers should be trained to deal with cyber incidents manually to protect the system and to reduce damage to equipment.

At the same time, efforts on enhancing cybersecurity awareness have been witnessed with growing importance. BIMCO (2018) argued that the maritime industry lacks a cyber awareness culture and governance, and this could increase its vulnerability and, thus, cause more cyber-attack incidents. Furthermore, shipping companies are required to develop cybersecurity management systems to urge cybersecurity awareness (IMO, 2017b).

2. To address human errors in cybersecurity, software can help reduce threats. 'Accessing links from suspicious emails (Ma1)', 'Downloading attached files from unknown emails (Ma2)' and 'Connecting USB or removable media to a computer without virus check (Ma3)' have been identified as top threats in this study. These could be well prevented by software. For example, installing and regularly updating anti-virus software have shown significant effectiveness in reducing cybersecurity risks. This can stop malicious programmes from being downloaded, and also from being executed. This is supported by the recommendation of BIMCO (2018) that an anti-virus programme should be installed on all work-related computers on board to reduce the possibility of cyberattacks. It also reports that the

number of maritime cyber incidents increased notably due to lack of software maintenance and patching. It is unavoidable to encounter various viruses and malicious programmes with the development of advanced technologies applied in the maritime industry. Shipping companies should pay particular attention to updating and upgrading their IT and OT systems to deal with the high-ranked threats from this paper and hence to ensure their competitiveness.

6. Conclusions

This research conducts a risk assessment of maritime cybersecurity. A list of cyber threats and cyber threat categories are identified and analysed through literature review and validated by both occurred accidents and maritime experts. A first-run questionnaire (Questionnaire 1) is conducted to screen the important cyber threats under each cyber threat category. A list of 21 threats are then further assessed through a second questionnaire (Questionnaire 2). A hybrid method combining FMEA and RBN is applied to analyse the risk criticality of cyber threats and their categories, and to assess maritime cybersecurity threats. The results of the analysis show that 'Malware' is the most critical threat category, followed by 'Phishing' and 'Human factor'. This research shows that 'Accessing links from suspicious emails' is the threat with the highest associated risk, followed by 'Connecting USB or removable media to a computer without virus check', and 'Downloading attached files from unknown emails'. Furthermore, a sensitivity analysis is used to validate the proposed BN model and investigate the impact of a single threat on the entire model. Finally, a list of measures to address maritime cyber threats is put forward, including education for new staff and regular training for all staff, installing anti-virus software, updating software regularly, implementing strong password policy, enhancing cybersecurity awareness, and applying web and email content filtering and proxy server.

The main contributions of this research are fourfold. First, this research aids to identify a list of maritime cyber threats. Based on their characteristics, it groups them into six categories, including 'Phishing', 'Malware', 'Man-in-the-middle attack', 'Theft of credential', 'Human factor', and 'Using outdated IT systems' (see Table 7). This categorised structure is also validated by a number of maritime experts (see Table 8). Second, this research proposes a BN model for maritime cybersecurity risk analysis (see Fig. 1). The proposed BN model is new and generic and hence can be further expanded to include more threats and/or categories (such as political risks, terrorism, piracy attacks, etc.). It thus provides a new direction for future research. Third, this research assesses the criticality of the proposed cyber threats (see Table 9). Through the results of this research, maritime managers are now aware of which cyber threats and categories are relatively security critical and thus where they should focus their efforts especially given restricted budgets. For academia, the findings highlight the crucial maritime cyber threats for future research to conduct a more in-depth analysis of these threats. Finally, this research explores several measures to address maritime cyber threats (see Section 5). Although these measures are not discussed against specific cyber threats, they can be widely applied to address various threats. In addition, our proposed measures are an area where future research could be focused on.

In the meantime, a few limitations could be addressed in future research. First, the number of responses could have been higher. The response rate to our questionnaires was around 40%; this is probably because the questionnaires (especially the second one) are complicated and not easy to be answered. Although the results are tested to be reliable and insightful, a higher number of responses could lead to new perspectives.

Second, although all respondents have some experience related to cybersecurity issues, one might argue that higher confidence should be placed on more experienced experts. Future research could weigh the expert opinion based on the level of familiarity with maritime cybersecurity and years of experience. On the other hand, one might argue that younger (and thus less experienced) domain experts might be more cybersecurity aware as younger groups are more familiar with modern IT systems. An interesting finding of our analysis is that junior respondents have a higher mean value in most cyber threat estimates compared to that of senior experts. This can be a notable insight for seafarers' training and company managers should pay more attention to enhancing the cybersecurity awareness of more senior staff. Future research can also address the risk perception of different respondents' backgrounds (e.g., based on their position, department, education, work experience, etc.) through the use of statistics such as *t*-test or Analysis of variance (ANOVA) models. The finding will provide further justification for the implementation of different control measures with regards to various stakeholder groups.

Furthermore, threats related to onboard systems are not always the same as those related to office computers; there are also differences in the network design and systems used in administration offices and those, say, in ports. Similarly, the consequences of an attack on a small shipping company are not the same as those of a similar attack on a large company, an international organisation or a governmental office. To address these differences, a more target-specific approach could be used. In this case, the assessed threats should be more carefully selected and should be more specific to the targeted systems and stakeholder groups.

Finally, this research mainly focuses on identifying and, more importantly, assessing the importance of cyber threats in the maritime industry. Several general measures are proposed to deal with cyber threats, but further research is required from the perspectives of the evaluation of measures to reduce the risk and select the most cost-effective ones for cybersecurity and resilience in the maritime industry.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that has been used is confidential.

Acknowledgements

This work is partially supported by IAMU (YAS FY 2019) and the EU H2020 ERC Consolidator Grant program (TRUST Grant No. 864724).

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.ocecoaman.2023.106480.

References

ABS, 2016. Guidance note on; the aplicaton of cybersecurity Principles to marine and offshore operations [online] Available at: https://maritimesafetyinnovationlab.org/wp-content/uploads/2016/09/abs-guidance-on-the-application-of-cyber-security-principles-2016_09.pdf. (Accessed 28 December 2021).

Alcaide, J.I., Llave, R.G., 2020. Critical infrastructures cybersecurity and the maritime sector. Transport. Res. Procedia 45, 547–554. https://doi.org/10.1016/j.trpro.2020.03.058.

Alyami, H., Yang, Z., Riahi, R., Bonsall, S., Wang, J., 2019. Advanced uncertainty modelling for container port risk analysis. Accid. Anal. Prev. 123, 411–421. https://doi.org/10.1016/j.aap.2016.08.007.

Androjna, A., Brcko, T., Pavic, I., Greidanus, H., 2020. Assessing cyber challenges of maritime navigation. J. Mar. Sci. Eng. 8 (10), 776. https://doi.org/10.3390/jmse8100776.

Asllani, A., Lari, A., Lari, N., 2018. Strengthening information technology security through the failure modes and effects analysis approach. Int. J. Qual. Innovat. 4 (1), 1–14. https://doi.org/10.1186/s40887-018-0025-1.

Ben Farah, M.A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., Bellekens, X., 2022. Cyber security in the maritime industry: a systematic survey of

recent advances and future trends. Information 13 (1), 22. https://doi.org/10.3390/info13010022.
BIMCO, 2016. The Guidelines on Cyber Security Onboard Ships, vol. 2 [online]. Available at: https://www.maritimeglobalsecurity.org/media/1014/c-users-jpl-onedrive-bimco-desktop-guidelines_on_cyber_security_onboard_ships_version_2-0_july2017.pdf. (Accessed 28 December 2021).
BIMCO, 2018. The Guidelines on cyber Security onboard ships. *Version 4* [online]. Available at: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships. (Accessed 28 December 2021).
Bolbot, V., Theotokatos, G., Boulougouris, E., Vassalos, D., 2020. A novel cyber-risk assessment method for ship systems. Saf. Sci. 131, 104908 https://doi.org/10.1016/j.ssci.2020.104908.
September Boyce, M.W., Duma, K.M., Hettinger, L.J., Malone, T.B., Wilson, D.P., Lockett-Reynolds, J., 2011. Human performance in cybersecurity: a research agenda, 1. In: Proceedings of the Human Factors *and Ergonomics Society Annual Meeting*, vol. 55. Sage CA, *Los* Angeles, CA, pp. 1115–1119. https://doi.org/10.1177/107118131155123. SAGE Publications.
Boyes, H., Isbell, R., 2017. Code of Practice: Cyber Security for Ships. Institution of Engineering and Technology.
Campisi, T., Marinello, S., Costantini, G., Laghi, L., Mascia, S., Matteucci, F., Serrau, D., 2022. Locally integrated partnership as a tool to implement a Smart Port Management Strategy: the case of the port of Ravenna (Italy). Ocean Coast Manag. 224, 106179 https://doi.org/10.1016/j.ocecoaman.2022.106179.
Caponi, S.L., Belmont, K.B., 2015. Maritime cybersecurity: a growing threat goes unanswered. Intellect. Property Technol. Law J. 27 (1), 16.
Chang, C.-H., Kontovas, C., Yu, Q., Yang, Z., 2021. Risk Assessment of the Operations of Maritime Autonomous Surface Ships, vol. 207. Reliability Engineering & System Safety. https://doi.org/10.1016/j.ress.2020.107324.
Chang, C.H., Xu, J., Song, D.P., 2015. Risk analysis for container shipping: from a logistics perspective. Int. J. Logist. Manag. 26 (1), 147–171. https://doi.org/10.1108/IJLM-07-2012-0068.
Chen, P., Zhang, Z., Huang, Y., Dai, L., Hu, H., 2022. Risk assessment of marine accidents with Fuzzy Bayesian Networks and causal analysis. Ocean Coast Manag. 228, 106323 https://doi.org/10.1016/j.ocecoaman.2022.106323.
CMACGM, 2020. Cyberattack update 10/11/2020 [online]. Available at: https://www.cmacgm-group.com/en/news-media/global-it-update-09-29-2020.
Coventry, L., Branley, D., 2018. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas 113, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008.
DNVGL, 2016. Cyber security resilience management for ships and mobile offshore units in operation [online]. Available at: https://cybersail.org/wp-content/uploads/2017/02/DNV-Cyber-Recommended-Practice-Ships-Mobile-Offshore-Units.pdf. (Accessed 28 December 2021).
Fan, S., Blanco-Davis, E., Yang, Z., Zhang, J., Yan, X., 2020. Incorporation of human factors into maritime accident analysis using a data-driven Bayesian network. Reliab. Eng. Syst. Saf. 203, 107070 https://doi.org/10.1016/j.ress.2020.107070.
Haseeb, J., Mansoori, M., Welch, I., 2021. Failure modes and effects analysis (FMEA) of honeypot-based cybersecurity experiment for IoT. October. In: 2021 IEEE 46th Conference on L*ocal Computer Networks (LCN)*. IEEE, pp. 645–648. https://doi.org/10.1109/LCN52139.2021.9525010.
Hassan, S., Wang, J., Kontovas, C., Bashir, M., 2022. Modified FMEA hazard identification for cross-country petroleum pipeline using Fuzzy Rule Base and approximate reasoning. J. Loss Prev. Process. Ind. https://doi.org/10.1016/j.jlp.2021.104616.
Heij, C., Knapp, S., 2018. Predictive power of inspection outcomes for future shipping accidents–an empirical appraisal with special attention for human factor aspects. Marit. Pol. Manag. 45 (5), 604–621. https://doi.org/10.1080/03088839.2018.1440441.
Hopcraft, R., Martin, K.M., 2018. Effective maritime cybersecurity regulation–the case for a cyber code. J. Indian Ocean Reg. 14 (3), 354–366. https://doi.org/10.1080/19480881.2018.1519056.
IMO, 2017a. MSC-FAL.1/Circ.3 [online] Available at: https://www.gard.no/Content/23896593/MSC-FAL.1-Circ.3.pdf. (Accessed 28 December 2021).
Hossain, N.U.I., Nur, F., Hosseini, S., Jaradat, R., Marufuzzaman, M., Puryear, S.M., 2019. A Bayesian network based approach for modeling and assessing resilience: a case study of a full service deep water port. Reliab. Eng. Syst. Saf. 189, 378–396. https://doi.org/10.1016/j.ress.2019.04.037.
IMO, 2017b. MSC 428 (98) [online]. Available at: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx. (Accessed 28 December 2021).
Imran, Z., Nizami, R., 2011. Advance secure login. Int. J. Sci. Res. Publ. 1 (1), 1–4.
Jones, K.D., Tam, K., Papadaki, M., 2016. Threats and impacts in maritime cyber security. Eng. Technol. Ref. 1 (1) https://doi.org/10.1049/etr.2015.0123.
Jones, B., Jenkinson, I., Yang, Z., Wang, J., 2010. The use of Bayesian network modelling for maintenance planning in a manufacturing industry. Reliab. Eng. Syst. Saf. 95 (3), 267–277. https://doi.org/10.1016/j.ress.2009.10.007.
Kanwal, K., Shi, W., Kontovas, C., Yang, Z., Chang, C.H., 2022. Maritime Cybersecurity: Are Onboard Systems Ready? Maritime Policy & Management, pp. 1–19. https://doi.org/10.1080/03088839.2022.2124464.
Karahalios, H., 2020. Appraisal of a Ship's Cybersecurity efficiency: the case of piracy. J. Transportat. Secur. 13 (3), 179–201. https://doi.org/10.1007/s12198-020-00223-1.
Karim, M.S., 2020. Australia's engagement in the international maritime organisation for indo-pacific maritime security. Ocean Coast Manag. 185 https://doi.org/10.1016/j.ocecoaman.2019.105032, 105032.
Kennedy, G.A.L., Shirvani, F., Scott, W.R., Campbell, A.P., 2021. Extending model-based approaches to integrate human factors aspects into cybersecurity and safety assessments. In: CORE 2021: Collaborating to Master Complexity: Conference on Railway Excellence, pp. 21–23. June 2021, Perth, WA, Australia.
Khan, R.U., Yin, J., Mustafa, F.S., Anning, N., 2021. Risk assessment for berthing of hazardous cargo vessels using Bayesian networks. Ocean Coast Manag. 210, 105673 https://doi.org/10.1016/j.ocecoaman.2021.105673.
Khan, S.K., Shiwakoti, N., Stasinopoulos, P., 2022. A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles. Accid. Anal. Prev. 165, 106515 https://doi.org/10.1016/j.aap.2021.106515.
Kovacs, E., 2020. *UN Maritime Agency Hit by 'Sophisticated Cyberattack* [online] Available at: https://www.securityweek.com/un-maritime-agency-hit-sophisticated-cyberattack. (Accessed 28 December 2021).
Lezzi, M., Lazoi, M., Corallo, A., 2018. Cybersecurity for Industry 4.0 in the current literature: a reference framework. Comput. Ind. 103, 97–110. https://doi.org/10.1016/j.compind.2018.09.004.
Lu, J., Su, W., Jiang, M., Ji, Y., 2022. Severity prediction and risk assessment for non-traditional safety events in sea lanes based on a random forest approach. Ocean Coast Manag. 225, 106202 https://doi.org/10.1016/j.ocecoaman.2022.106202.
Mallik, A., 2019. Man-in-the-middle-attack: understanding in simple words. Cyberspace: J. Pendidik. Teknol. Info. 2 (2), 109–134. https://doi.org/10.22373/cj.v2i2.3453.
Markit, I., 2016. 2016 cyber security survey in association with BIMCO [online] Available at: https://cybersail.org/wp-content/uploads/2017/02/IHS-BIMCO-Survey-Findings.pdf. (Accessed 28 December 2021).
Markit, I., 2018. Maritime cyber survey 2018 - the results [online] Available at: https://bi-cd02.bimco.org/-/media/bimco/news-and-trends/news/security/cyber-security/2018/fairplay-and-bimco-maritime-cyber-security-survey-2018.ashx. (Accessed 28 December 2021).
Mazzarolo, G., Jurcut, A.D., 2019. Insider threats in Cyber Security: The enemy within the gates. arXiv preprint arXiv:1911.09575. 10.48550/arXiv.1911.09575.
Meland, P.H., Bernsmed, K., Wille, E., Rødseth, Ø.J., Nesheim, D.A., 2021. A retrospective analysis of maritime cyber security incidents. TransNav: Int. J. Mar. Navigat. Saf. Sea Transportat. 15 https://doi.org/10.12716/1001.15.03.04.
Mraković, I., Vojinović, R., 2019. Maritime cyber security analysis–how to reduce threats? Trans. Marit. Sci. 8, 132–139. https://doi.org/10.7225/toms.v08.n01.013, 01.
Park, C., Shi, W., Zhang, W., Kontovas, C.A., Chang, C.H., 2019. Evaluating cybersecurity risks in the maritime industry: a literature review. November. In: Proceedings of the International Association of Maritime Universities (IAMU) Conference.
Pham, D.V., Halgamuge, M.N., Syed, A., Mendis, P., 2010. Optimizing windows security features to block malware and hack tools on USB storage devices. In: Progress in Electromagnetics Research Symposium.
Progoulakis, I., Rohmeyer, P., Nikitakos, N., 2021. Cyber physical systems security for maritime assets. J. Mar. Sci. Eng. 9 (12), 1384. https://doi.org/10.3390/jmse9121384.
Qbeitah, M.A., Aldwairi, M., 2018. Dynamic Malware Analysis of Phishing Emails. *2018 9th International Conference On Information And Communication Systems (ICICS)*of Conference. https://doi.org/10.1109/IACS.2018.8355435.
Ren, A., Wu, D., Zhang, W., Terpenny, J., Liu, P., 2017. Cyber security in smart manufacturing: survey and challenges. In: IIE Annual Conference. Proceedings. Institute of Industrial and Systems Engineers (IISE), pp. 716–721.
Ren, J., Jenkinson, I., Wang, J., Xu, D., Yang, J., 2008. A methodology to model causal relationships on offshore safety assessment focusing on human and organizational factors. J. Saf. Res. 39 (1), 87–100. https://doi.org/10.1016/j.jsr.2007.09.009.
Sen, R., 2016. Cyber and Information Threats to Seaports and Ships. Maritime Security, pp. 281–302. https://doi.org/10.1016/B978-0-12-803672-3.00009-1.
Senarak, C., 2021. Port cybersecurity and threat: a structural model for prevention and policy development. Asian J. Shipp. Logist. 37 (1), 20–36. https://doi.org/10.1016/j.ajsl.2020.05.001.
Shead, S., 2021. South Africa port operations halted and workers reportedly put on leave after major cyberattack. *CNBC* [online], Available at: https://www.cnbc.com/2021/07/27/transnet-halts-port-operations-in-south-africa-after-major-cyberattack.html. (Accessed 16 December 2021).
Suciu, G., Scheianu, A., Petre, I., Chiva, L., Bosoc, C.S., 2019. Cybersecurity threats analysis for airports. April. In: World Conference on Information *Systems And Technologies*. Springer, *Ch*am, pp. 252–262.
Svilicic, B., Kamahara, J., Rooks, M., Yano, Y., 2019. Maritime cyber risk management: an experimental ship assessment. J. Navig. 72 (5), 1108–1120. https://doi.org/10.1017/S0373463318001157.
Tam, K., Jones, K., 2019. MaCRA: a model-based framework for maritime cyber-risk assessment. WMU J. Marit. Aff. 18 (1), 129–163. https://doi.org/10.1007/s13437-019-00162-2.
Tusher, H.M., Munim, Z.H., Notteboom, T.E., Kim, T.E., Nazir, S., 2022. Cyber security risk assessment in autonomous shipping. Marit. Econ. Logist. 24, 208–227. https://doi.org/10.1057/s41278-022-00214-0.
Uusitalo, L., 2007. Advantages and challenges of Bayesian networks in environmental modelling. Ecol. Model. 203 (3–4), 312–318. https://doi.org/10.1016/j.ecolmodel.2006.11.033.
Wan, C., Yan, X., Zhang, D., Qu, Z., Yang, Z., 2019a. An advanced fuzzy Bayesian-based FMEA approach for assessing maritime supply chain risks. Transport. Res. E Logist. Transport. Rev. 125, 222–240. https://doi.org/10.1016/j.tre.2019.03.011.
Wan, C., Yan, X., Zhang, D., Yang, Z., 2019b. Analysis of risk factors influencing the safety of maritime container supply chains. Int. J. Shipp. Transp. Logist. (IJSTL) 11 (6), 476–507. https://doi.org/10.1504/IJSTL.2019.103872.
Wan, C., Tao, J., Yang, Z., Zhang, D., 2022. Evaluating recovery strategies for the disruptions in liner shipping networks: a resilience approach. Int. J. Logist. Manag. 33 (2), 389–409. https://doi.org/10.1108/IJLM-05-2021-0263.

Yang, Y., Zhong, M., Yao, H., Yu, F., Fu, X., Postolache, O., 2018. Internet of things for smart ports: technologies and challenges. IEEE Instrum. Meas. Mag. 21 (1), 34–43. https://doi.org/10.1109/MIM.2018.8278808.

Yang, Z., Bonsall, S., Wang, J., 2008. Fuzzy rule-based Bayesian reasoning approach for prioritization of failures in FMEA. IEEE Trans. Reliab. 57 (3), 517–528. https://doi.org/10.1109/TR.2008.928208.

Yeboah-Boateng, E.O., Amanor, P.M., 2014. Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. J. Emerg. Trends Comput. Inf. Sci. 5 (4), 297–307.

Yoo, Y., Park, H.S., 2021. Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. J. Mar. Sci. Eng. 9 (6), 565. https://doi.org/10.3390/jmse9060565.

Yu, Q., Liu, K., Chang, C.-H., Yang, Z., 2020. Realising advanced risk assessment of vessel traffic flows near offshore wind farms. Reliab. Eng. Syst. Saf. 203, 107086 https://doi.org/10.1016/j.ress.2020.107086.

Zhou, Y., Li, X., Yuen, K.F., 2022. Holistic risk assessment of container shipping service based on Bayesian Network Modelling. Reliab. Eng. Syst. Saf. 220, 108305 https://doi.org/10.1016/j.ress.2021.108305.