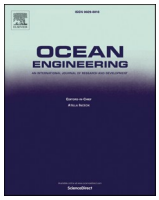
Ocean Engineering 312 (2024) 119078

Contents lists available at ScienceDirect

Ocean Engineering

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



Research paper

Decoding dependencies among the risk factors influencing maritime cybersecurity: Lessons learned from historical incidents in the past two decades

Massoud Mohsendokht [a], Huanhuan Li [a,*], Christos Kontovas [a], Chia-Hsun Chang [a], Zhuohua Qu [b], Zaili Yang [a,**]

[a] Liverpool Logistics, Offshore and Marine (LOOM) Research Institute, Liverpool John Moores University, Liverpool, UK
[b] Liverpool Business School, Liverpool John Moores University, UK

ARTICLE INFO

Keywords:
Maritime security
Cyber-attacks
Bayesian network
Risk analysis
Cybersecurity

ABSTRACT

The distinctive features of maritime infrastructures present significant challenges in terms of security. Disruptions to the normal functioning of any part of maritime transportation can have wide-ranging consequences at both national and international levels, making it an attractive target for malicious attacks. Within this context, the integration of digitalization and technological advancements in seaports, vessels and other maritime elements exposes them to cyber threats. In response to this critical challenge, this paper aims to formulate a novel cybersecurity risk analysis method for ensuring maritime security. This approach is based on a data-driven Bayesian network, utilizing recorded cyber incidents spanning the past two decades. The findings contribute to the identification of highly significant contributing factors, a meticulous examination of their nature, the revelation of their interdependencies, and the estimation of their probabilities of occurrence. Rigorous validation of the developed model ensures its robustness for both diagnostic and prognostic purposes. The implications drawn from this study offer valuable insights for stakeholders and governmental bodies, enhancing their understanding of how to address cyber threats affecting the maritime industry. This knowledge aids in the implementation of necessary preventive measures.

1. Introduction

Global maritime transport is crucial, accounting for over 80% of global trade in goods (Li and Yang, 2023; UNCTAD, 2022). The extensive use of advanced technology and intelligent telecommunication systems in both mobile and fixed maritime components raises significant concerns about the potential impact of cyber-attacks. In the contemporary era, seaports and vessels employ a diverse range of sophisticated technological systems that incorporate electronic software and hardware to improve effectiveness, safety, and overall functionality. The implementation of Automated Terminal Operating Systems (ATOS) for container optimization, Port Security Systems, and Cargo Handling Equipment Automation in seaports, along with Global Positioning Systems (GPS), Automated Identification Systems (AIS), and Electronic Chart Display and Information Systems (ECDIS) on vessels (Weng et al., 2023), raises concerns regarding cybersecurity in the maritime domain. In 2017, Maersk, a leading global shipping company with the largest fleet capacity (comprising 18% of the global fleet capacity), experienced significant financial losses amounting to $300 million due to the most severe cyberattack ever recorded in the maritime industry. The attack involved the NotPetya ransomware, which infiltrated the company's reservation system, resulting in the widespread congestion of 80 ports worldwide. Some of these ports experienced complete disruptions in loading traffic and container operations. Rotterdam's automated terminal was rendered inactive, and electronic systems in New York and New Jersey froze (Benmalek, 2024). Given the gravity of cyber-attacks and their unique nature, which sets them apart from other security concerns by transcending physical boundaries, hackers have the freedom to target electronic systems worldwide at any given moment.

Recognizing this, there is an essential need to redirect attention from conventional safety and security measures on physical systems toward addressing the risks posed by cyber threats. In 2022, the International

* Corresponding author.
** Corresponding author.
E-mail addresses: h.li2@ljmu.ac.uk (H. Li), z.yang@ljmu.ac.uk (Z. Yang).

https://doi.org/10.1016/j.oceaneng.2024.119078
Received 10 July 2024; Received in revised form 16 August 2024; Accepted 24 August 2024
Available online 29 August 2024
0029-8018/© 2024 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

Maritime Organization (IMO) took a significant step by revising its guidelines on "Maritime Cyber Risk Management". These updated guidelines offer comprehensive recommendations at a high level, aiming to protect the shipping industry from both existing and evolving cyber threats and vulnerabilities. Notably, the guidelines incorporate functional elements designed to enhance the efficacy of cyber risk management practices in the maritime sector (IMO, 2022). On an individual level, attempts have been made to assess the cybersecurity risks in the maritime sector through both qualitative and quantitative approaches. Oruc et al. (2022) presented a summary of global standards, current bridge test environments, and regulations established by the IMO for evaluating cybersecurity risks in integrated navigation systems. Kessler (2021) offered a technical analysis of Control Area Network (CAN) bus standards and operations within maritime vessels, delving into cybersecurity vulnerabilities that could compromise the confidentiality, integrity, or availability of information in the maritime industry. Schinas and Metzger (2023) conducted a review highlighting policy gaps in the realm of cybersecurity within the maritime domain. In response to these identified gaps, they introduced the concept of "cyber-seaworthiness" as a proposed solution. Kanwal et al. (2022) conducted an evaluation examining the interplay between the cybersecurity performance of ships and six distinct cybersecurity dimensions. These dimensions encompassed aspects such as "regulations," "company procedures," "shipboard system readiness," "training and awareness," "human factor," and "compliance monitoring".

From a quantitative perspective, attempts have been made to apply conventional risk assessment techniques to address cyberthreats. Examples of such efforts include the use of HAZOP (Hazard and Operability), FMEA (Failure Mode and Effect Analysis), FTA (Fault Tree Analysis), ETA (Event Tree Analysis), Bow-tie, attack trees, and risk matrices (Henriques De Gusmão et al., 2018; Komal, 2023; Progoulakis et al., 2021; Yoo and Park, 2021). However, the primary challenge with these approaches lies in the significant uncertainty inherent in data analysis, raising questions about their effectiveness. To address this concern, some researchers have proposed the adoption of advanced methods like Bayesian Networks (BN) or a combination of BN with the traditional approaches mentioned earlier. This integration is exemplified in the work of Park et al. (2023), who utilized a combination of FMEA and Rule-based BN (RBN) to assess and prioritize the risk levels associated with various cyber-attacks. Despite some improvement in cybersecurity analysis through these recent methodologies, a drawback is their reliance on subjective data. The collection of data predominantly relies on expert judgment, a practice that invites debate due to inherent biases in expert opinions. Factors such as the number of experts responding to questionnaires and the quality of their responses critically determine the study's reliability. Additionally, the weighting assigned to experts and their opinions is a point of contention. While in safety and security analyses, greater weight is often given to experts with more experience, in the realm of cyberthreats, there is an argument that younger experts, possessing greater familiarity with Information Technology (IT) systems, may offer more realistic insights (Öğütçü et al., 2016). Basically, the existing maritime cybersecurity analysis methods at large rely on subjective and/or qualitative analysis (e.g., Park et al.'s hybrid FMEA (Park et al., 2023) due to the constraints of data availability. Therefore, in Park et al.'s work (Park et al., 2023), the risk parameters are generic at a macro level, such as likelihood and consequence severity that could be evaluated by domain experts. Additionally, a detailed classification of cyber threats across different maritime sectors is lacking. In contrast, in this study, it is for the first time to employ micro-level risk factors (e.g., regions, attack modes, vulnerable targets) to quantify maritime cybersecurity risk levels. It can therefore better reflect the real-world cyber security threats and evaluate/predict their risk levels, as revealed by the implications of the work.

Taking into account the limitations identified in prior research, this paper endeavors to pioneer a novel approach to maritime cybersecurity risk analysis. The proposed method involves harnessing real data encompassing all cyber incidents within the maritime industry over the past two decades. The intention is to employ this comprehensive dataset to train a data-driven BN model, offering a more robust and empirically grounded framework for evaluating cybersecurity risks in the maritime sector. The contributions of this paper can be summarized as follows:

- Comprehensive data collection on maritime cybersecurity: An exhaustive collection of recorded cyber-attacks within the maritime industry was conducted, and the data was refined to develop a new dataset that encompasses comprehensive information on the most relevant risk factors.
- Novel diagnosis analysis: This paper introduces a pioneering approach to quantifying maritime cybersecurity risk analysis by utilizing real data spanning two decades to train a data-driven BN model. This enhances the empirical foundation of cybersecurity risk assessment in the maritime sector and marks the first significant improvement in the accuracy of cybersecurity diagnosis analysis.
- Identification of contemporary patterns: This study contributes to tracking contemporary patterns in maritime cyber-attacks, elucidating key influencing factors such as vulnerable targets, affected countries, high-risk regions, types of cyber-attacks, and their origins.
- Insights for nuanced understanding: The adopted approach offers valuable insights for a nuanced comprehension of the dynamics surrounding maritime cyber threats, providing a more comprehensive perspective. The results serve as a benchmark for enhancing diagnostic analyses, ultimately leading to improved prediction accuracy.
- Implications for stakeholders and governmental bodies: The study's implications provide valuable insights for stakeholders and governmental bodies, enriching their understanding of addressing cyber threats in the maritime industry. This includes optimized resource allocation, preventive measures, and mitigation strategies.

The following sections of the paper are structured as follows: Section 2 offers a brief critique of existing literature on maritime cybersecurity and studies related to data-driven BN risk analysis. In Section 3, the paper delves into the details of the data collection process, methodology, and validation techniques employed for the developed model. Section 4 presents the analysis results and engages in discussions regarding the model's outputs. Further discourse on the results and their potential implications, along with considerations for future research directions, is provided in Section 5. The paper concludes in Section 6 by drawing overall insights and summarizing key findings.

2. Literature review

2.1. Studies on cybersecurity risk assessment

Examining the literature pertaining to cyber-attacks, a significant portion of the published papers originates from the fields of computer security and related disciplines (Berghout and Benbouzid, 2022; Diao, 2024; Patriarca et al., 2022; Tang et al., 2023). However, when focusing on the maritime field, there is a limited number of identified papers, indicating a substantial gap requiring additional research. Several review papers (Ashraf, 2022; Ben Farah, 2022; Larsen and Lund, 2021; Tusher et al., 2022) offer a thorough overview of published papers on maritime cybersecurity, with the work by Bolbot et al. (2022) standing out as the most comprehensive among them. To narrow the focus to papers employing a risk assessment methodology, the emphasis will be on studies involving risk identification, evaluation, and analysis.

Additionally, attention will be given to research that develops frameworks and conducts vulnerability analyses within this domain. Several contributions in the realm of cybersecurity studies can be attributed to model-based approaches. Tam and Jones (2019), for instance, introduced a model-based framework named 'MaCRA'

(Maritime Cyber Risk Analysis). This framework aims to identify primary risk outcomes, attackers, attack vectors, and systems that would benefit or require additional security. Moreover, it seeks to characterize the severity of maritime cyber risks and, crucially, to present risk data in informative views that aid human decision-making processes. Schauer et al. (2019) introduced a six-stage methodology named 'MITIGATE SCRA', utilizing a graph-based approach to analyze the risk of cyber-attacks within the maritime supply chain. Carreras Guzman et al. (Carreras Guzman et al., 2020) presented a master model diagram that features a multi-layered diagrammatic representation of cyber-physical systems. This model is designed for a comprehensive safety and security risk analysis, showcasing its application in the maritime sector through the analysis of an autonomous surface vehicle. In the realm of quantitative cyber threat risk assessment, notable work includes the following: Park et al. (2023) introduced an innovative hybrid framework, combining FMEA with a rule-based BN approach. This framework was developed to assess the risk levels of various cyber-attacks in maritime operations and rank them accordingly. Quantitative data for this assessment was gathered through a questionnaire and expert judgments, contributing to a robust understanding of cyber threat risks. A similar study in the realm of quantifying cyber threat risks was undertaken by Uflaz et al. (2024), focusing on the assessment of potential cyber-attacks on bridge navigational systems. Their approach involved a combination of Failure Modes, Effects, and Criticality Analysis (FMECA), expert judgment, Dempster-Shafer theory, and a rule-based BN technique. This comprehensive methodology aimed to provide a quantitative evaluation of the risks associated with cyber threats on bridge navigational systems. In terms of the port sector, Gunes et al. (2021) proposed a cyber security risk assessment methodology tailored for seaports. Their approach involved simulating four distinct cyber-attack scenarios within a designated container port. Employing a comprehensive 13-stage framework, they quantified the risk associated with each scenario on a scale ranging from 1 to 10. This systematic assessment provided a nuanced understanding of cyber security risks specific to seaport environments.

2.2. Application of BN in maritime risk assessment

Among the array of methodologies discussed for assessing the risks posed by cyber-attacks, BN stands out for its exceptional ability to model and manage uncertainty effectively. When compared to conventional risk assessment approaches such as FTA, FMEA, and risk matrices, BN emerges as superior in its capacity to capture the intricate causal relationships among risk factors. It excels in managing both subjective and objective data concurrently. Moreover, in terms of scalability, recent advancements in computational techniques have empowered BN to handle the construction and analysis of large-scale structures (Cheng, 2024; Kong et al., 2024; Sheng et al., 2024). This progress facilitates the modeling of complex systems with myriad interconnected variables. Additionally, in relation to adaptability, BN offers the flexibility to be updated and refined with emerging data or evolving system insights. This feature ensures that risk assessments remain pertinent and up to date over time (Kabir and Papadopoulos, 2019). These inherent characteristics position BN as a promising and effective tool for the analysis of cyber-attacks, enabling comprehensive modeling and the study of their potential consequences. In this context, initiating the deployment of such a methodology begins with the structural learning of the BN. Existing literature indicates that mastering the structure learning of BN can be a formidable task, given the super-exponential multitude of potential graphs and the challenge of accurately diagnosing relationships among various nodes. The integration of expert knowledge has the potential to enhance the learning process, particularly when the number of experts and their level of experience reach a satisfactory threshold. In this regard, leveraging experts' insights into cause-effect relationships can be employed to shape the network's structure. Furthermore, modeling the individual probabilities of experts correctly labeling the inclusion or exclusion of edges can be employed to refine and improve the overall learning algorithm (Amirkhani et al., 2017). Given the wealth of literature on the application of BN in maritime risk, a selection strategy is implemented to offer a manageable yet inclusive set of papers. This strategy involves picking a combination of both highly cited and recently published papers. These chosen papers should not only focus on maritime security but also offer innovative perspectives on the application of BN within this context. Both Bouejela et al. (Bouejla et al., 2014) and Pristrom et al. (2016) utilized expert judgment alongside data from the IMO to establish a BN structure for evaluating the risk of piracy attacks on ships. Jiang and Lu (2020) adopted a hybrid approach, combining statistical data with expert knowledge for BN structure learning, applying this methodology to analyze maritime piracy in Southeast Asia. Hao et al. (2023) introduced a risk analysis and prediction model that explores the internal dynamics of maritime piracy accidents using a combination of the Markov model and BN. Chang et al. (2021) conducted a risk assessment of autonomous ships with a hybrid method combining FMEA and BN. Tuncel et al. (Tunçel et al., 2024) devised an integrated approach incorporating rule-based BN and FMECA under evidential reasoning (ER) to assess the risks associated with anchoring operations on ships.

Although expert judgment is acknowledged as a valuable resource for BN structure learning, especially in scenarios with limited or unavailable data, it is essential to acknowledge the potential presence of uncertainty and biases. When abundant data is accessible, the utilization of machine learning algorithms becomes a precise and efficient alternative for learning the BN structure. With the latest progress in BN capabilities, integrating machine learning methods into BN can boost their predictive power and enable the management of complex datasets, thereby enhancing the precision of risk assessments. Furthermore, the integration of sophisticated techniques for quantifying and propagating uncertainty within BN has been devised, leading to more resilient and trustworthy risk assessments through the consideration of uncertainty in input variables and model parameters. This approach, referred to as data-driven BN, involves the extraction of causal relationships, dependencies, and interdependencies among risk factors directly from the available data. By leveraging the information contained in the data, this method offers a more objective and empirical way to establish the structure of the BN, particularly in situations where extensive datasets are available. The adoption of a data-driven approach is observable in numerous maritime risk assessment studies. In order to provide a representative array of papers concerning data-driven BN structure learning, a comparable approach is utilized, selecting a mix of both widely referenced and recently published works, all of which are represented in Table 1.

2.3. Research gaps

With consideration of the conducted literature review, the following research gaps have been revealed:

1) The dominance of conventional risk assessment techniques in cybersecurity: The majority of the existing literature relies on conventional risk assessment techniques (e.g., HAZOP, FMEA, FTA, ETA, Bowtie, attack trees, and risk matrices) to address cyber threats. However, these methods have been criticized due to the high uncertainty in cybersecurity risk data and the associated challenges in risk inference. There is a need for further research to adapt or improve risk analysis methods to enable them to handle the inherent uncertainty in cybersecurity data.
2) Subjectivity in expert judgment: The reliance on subjective data and expert judgment in most studies introduces potential biases, affecting the reliability of cyber risk assessments. New research should focus on finding ways to minimize these biases and enhance the objectivity of cybersecurity evaluations. It is essential to explore methods of mitigating expert bias in cybersecurity risk assessment.

Table 1
Summarization of data-driven BN approach in maritime risk analysis.

No.	Source	Amount of dataset	Number of nodes	Structure learning technique	Application
1	Fan et al. (Fan et al., 2020)	208	25	Tree Augmented Naïve (TAN) Bayes	Human factors in maritime accidents
2	Liu et al. (Liu et al., 2021)	414	20	Bayesian searching approach	Maritime major accident records in the Chinese coastal waters
3	Liu et al. (Liu et al., 2022)	1880	11	Bayesian searching approach	Port State Control inspection
4	Fan et al. (Fan et al., 2022)	61	25	TAN Bayes	Maritime accidents within restricted waters
5	Li et al. (Li et al., 2023)	428	23	TAN Bayes	Global maritime accident
6	Zhou et al. (Zhou et al., 2024)	402	24	TAN Bayes	maritime casualty analysis
7	Fan and Yang (Fan and Yang, 2024)	104	6	LASSO and TAN Bayes	Human fatigue investigation in maritime accidents
8	Xu et al. (Xu et al., 2024)	42418	18	Noisy-OR gate and the IF-THEN method	Navigation status control of cargo ships.
9	Wang and Yang (Wang and Yang, 2018)	350	21	Augmented naive Bayesian Networks	Accident severity in waterborne transportation
10	Kamal and Cakir (Kamal and Çakır, 2022)	418	13	TAN Bayes	Marine accidents in Istanbul Strait

3) Quality and weighting of expert opinions: Since most current studies rely on subjective data, leading to the ongoing debate about how to weigh expert opinions, particularly when balancing between the insights of experienced and less experienced experts. New research is needed to develop methods for systematically and fairly weighing expert opinions or to create alternative approaches that can effectively balance different types of expertise.
4) Comprehensive classification of cyber threats in different maritime sectors: Many existing studies on maritime cybersecurity risk analysis suffer from a lack of comprehensive classification of cyber threats across various maritime sectors. Some studies focus solely on cyber threats affecting vessels, while others concentrate only on shore-based entities. New research should aim to develop more granular and sector-specific classifications of cyber threats to improve the accuracy and relevance of risk assessments.
5) Real-world cybersecurity threat reflection: Many studies fail to adequately consider real-world cyber incidents within the industry, which can result in unrealistic objectives and less accurate outcomes. To address this gap, incorporating micro-level risk factors and developing an objective database based on historical data could provide a more accurate reflection of real-world threats. Research should further validate this approach by comparing the effectiveness of micro-level versus macro-level risk assessments in predicting and mitigating real-world cyber threats.

This paper builds on the existing literature by pioneering the use of data-driven learning in developing a BN model for analyzing cyber threats in the maritime sector. However, in contrast to prior research, it introduces a novel approach to analyzing the risks associated with maritime cyberattacks by incorporating objective data for the first time. To achieve this goal, two decades' worth of maritime cyber incidents are manually collected, analyzed and utilized to construct a BN model driven by machine learning. Additionally, a comprehensive manual examination of each maritime cybersecurity incident across diverse entities, including seaports, shipping companies, offshore installations, vessels, and others, is conducted to establish the inaugural maritime cybersecurity risk database. This study approaches the process from a broad and worldwide viewpoint, emphasizing its theoretical novelty. The research progresses through several phases, including data collection, model development, comparative analysis of models, validation of the model, and the resulting model output. In contrast to the traditional use of BN in risk assessment, this paper is among the pioneering ones investigating cyber security risk assessment, and it additionally proves the effectiveness of the developed model in maritime cybersecurity risk analysis, a less explored but crucial area of growing importance for safety at sea. It newly identifies the risk factors during the model comparison stage, using real-world data. This endeavor marks a substantial leap forward in the discipline, enhancing comprehension of maritime cyber-attacks and refining our understanding of the risk attributes linked to cyber threats within this field.

3. Methodology

This paper utilizes a data-driven BN methodology to pinpoint the 'Security Risk Influencing Factors' (SRIFs) related to cyber threats in maritime infrastructures such as seaports and vessels. In this regard, a holistic framework encompassing four pivotal stages is developed: data collection and processing, BN model construction, model validation and verification, analysis of model outputs, and extraction of useful information. The ultimate goal is to propose effective guidelines for bolstering maritime security. Fig. 1 demonstrates the entirety of our proposed methodology.

3.1. Data collection and processing

In the process of gathering information on cyber-attacks targeting maritime infrastructures, the Maritime Cyber Attack Database (MCAD) is employed for its specific focus (MCAD, 2023). Originating from open-source data, the MCAD is the result of collaborative efforts by the Maritime IT Security research group at NHL Stenden University of Applied Sciences in the Netherlands, encompassing details on more than 160 cyber incidents within the maritime sector. This database goes beyond vessel-related events, also documenting incidents affecting seaports and various maritime facilities on a global scale. The timeline for data collection spans from 2001 to 2023, allowing for a comprehensive analysis of maritime cyber threats and the identification of meaningful patterns over an extensive period. Upon thorough examination of the database and consideration of pertinent cases within the realm of maritime cyber-attacks, the decision was made to adopt a comprehensive approach. Given the novelty of the subject and the intricate interplay of cyber-attacks across diverse elements of the maritime industry, including the potential impact on seaports, it was determined that all incidents, irrespective of their specific target (seaports, ships, offshore structures, and related components), would be included for analysis. This inclusive approach ensures a holistic understanding of the various cyber threats within the maritime domain. Data collection involved manual extraction from the MCAD database, with categorization according to various SRIFs. However, during this process,

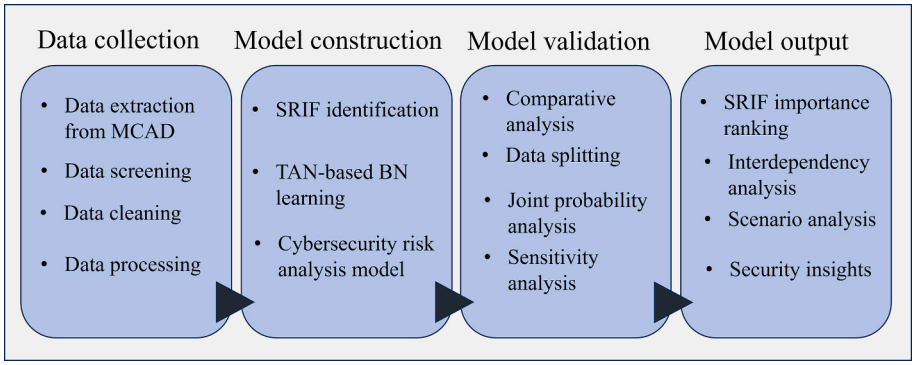


Fig. 1. The proposed framework for security risk analysis.

certain shortcomings were encountered in obtaining precise information regarding the SRIFs. These shortcomings stem from certain gaps in the data, such as missing details about the target characteristics (such as whether it was offshore infrastructure, a port, a shipping company, or a maritime organization), the extent of the consequences (whether the impact of the cyberattack was significant or minimal), the source of the attack (with some cases having unidentified origins in the database), and the geographical region of the incidents. Not all data were available in the database. To address these issues, additional information from news articles and public sources was researched and gathered to create a refined database suitable for model development. Each case was scrutinized individually to extract missing information through resources referenced by MCAD and cross-referencing relevant websites to validate the data in MCAD. For instance, in February 2022, the UK ferry operator Wightlink, based in Portsmouth, was hit by a cyber-attack. The database only mentioned that the back-office IT systems were compromised. Our further investigation revealed it was a phishing attack with a minor impact on the company's functionality. Another example is the June 2021 ransomware attack on the network of the Woods Hole, 'Martha's Vineyard, and Nantucket Steamship Authority in Boston, MA, USA. Initially, the database only mentioned that malware encrypted files, rendering the system inoperable. Additional research uncovered that the attack had a major impact, preventing changes or bookings for reservations, causing ticketing delays, and limiting the availability of credit card systems, necessitating cash transactions. Overall, the refined database underwent rigorous scrutiny and cross-checked with multiple information sources to ensure the reliability of the collected data and address any missing items in the MCAD.

3.2. SRIF identification

In this paper, the elements influencing the security of maritime infrastructures and vessels are denoted as SRIFs. These factors are identified by examining data from the MCAD, as well as by incorporating information from a literature review to classify and compile relevant indicators. The pertinent literature is chosen by conducting searches with keywords such as "cybersecurity", "cyberattacks," and "cyber threats" on the Web of Science. From numerous identified papers, 10 have been scrutinized for their relevance and content, with the aim of extracting the most significant SRIFs. Table 2 presents the selected literature along with their corresponding SRIFs.

In the context of cyber-attacks, the precise factors that exert a significant influence on the overall risk level are not yet fully understood due to their novel and complex nature. However, a literature review, as outlined in Table 2, and available historical data have identified 7 SRIFs for a data-driven BN analysis. These factors encompass cyber threats, target entities (including offshore structures, shipping companies, vessels, etc., not limited to seaports), victim and origin countries, regions, years, and consequences. It is noteworthy that the scope of potential targets extends beyond seaports to include various maritime-related elements. This broader perspective provides a holistic understanding of how cyber-attacks may unfold in the maritime industry. Throughout the selection process of SRIFs, several criteria were considered to ensure the model's accuracy, relevance, and practicality. Here are the key criteria adopted for this study:

1) Literature review: It is evident that SRIFs recognized in the literature as critical to cybersecurity should be prioritized. This process involves examining academic papers, industry reports, and case studies to identify factors with a significant impact on research outcomes. Furthermore, among the identified SRIFs, those empirically validated through previous studies are more likely to have a well-established relationship with the outcomes being modelled. Therefore, we conducted a comprehensive literature review by conducting searches with keywords such as "cybersecurity", "cyberattacks," and "cyber threats" on the Web of Science. From numerous identified

Table 2
The sources of SRIFs based on the retrieved results and the comprehensive dataset.

Reference	SRIFs											
	1	2	3	4	5	6	7	8	9	10	11	12
Uflaz et al. (2024)				*	*	*	*		*	*	*	
Gunes et al. (2021)			*	*	*	*	*		*	*	*	
Kavallieratos et al. (2021)					*	*			*	*		
Bolbot et al. (2020)			*	*	*	*	*	*	*	*	*	
Kavallieratos et al. (2019)					*	*	*			*	*	
Yoo and Park (2021)						*			*	*	*	
Park et al. (2023b)					*					*	*	
Tam and Jones (2019)			*	*	*	*	*	*	*	*	*	
Henriques De Gusmão et al. (2018)					*	*	*		*		*	
MCAD	*	*	*		*	*	*				*	*

Note: 1. Region; 2. Country; 3. Perpetrator; 4. Scenario; 5. Cyber-attack type; 6. Target; 7. Successful attack; 8. Property damage; 9. Prevention ability; 10. Security risk level; 11. Consequence; 12. Temporal trend.

Table 3
Cyber SRIFs states and their descriptions.

SRIFs	States	Description
Cyber threats	DDOS, Hacking, Jamming, Malware, Phishing, Ransomware, Spoofing	A "DDOS" which stands for Distributed Denial of Service attack, is an intentional effort to disrupt the normal operation of a network, service, or website by inundating it with a surge of internet traffic. "Hacking" serves as a broad term encompassing unauthorized access into computer or network systems, aiming to manipulate information, engage in data theft, or disrupt normal operations. "Jamming" refers to intentional interference with radio and GPS signals, wireless communications, or radar systems, with the goal of disrupting or preventing normal communication. "Malware" involves introducing harmful software to disrupt the functioning of computer systems, networks, or devices, leading to malfunctions or the dissemination of inaccurate data. "Phishing" is occurred when victims are deceived into revealing sensitive information through deceptive communication posing as a trustworthy entity. "Ransomware", evident from its name, is a form of virtual extortion in which malicious software encrypts the victim's system, rendering it inaccessible, and demands payment for the decryption key. "Spoofing" deceives AIS systems with false signals, causing incorrect vessel information, while the system remains operational; distinct from jamming, which disrupts and disables the system.
Target	Offshore structures, Port, Shipping company, Vessel, Other	"Offshore structures" encompass a range of installations and facilities situated in bodies of water, usually distant from the shore. Examples include gas and oil platforms, wind farms, and drilling rigs. "Shipping companies" are responsible for the sea transportation of goods or passengers. They own, operate, and manage vessels, including cargo ships, container ships, tankers, and more, facilitating global maritime trade and transportation. Entities related to maritime activities, including shipbuilding firms, energy distributors, insurance, and brokerage organizations situated on the shore, are categorized under the label "other."
Victim countries	Australia, Belgium, Canada, China, Cyprus, Denmark, Germany, Greece, India, Indonesia, Iran, Israel, Japan, Kuwait, Netherland, Norway, Philippines, Russia, Saudi Arabia, Singapore, South Korea, UK, Ukraine, USA, Other	"Countries" experiencing fewer than three cyber-attacks are collectively categorized under the "other" state. The screening criteria are established at fewer than 3 cyber-attacks to eliminate over 15 countries as new states. This method is adopted to circumvent the subsequent drawbacks: 1. As the quantity of states within a node rises, so does the complexity of the BN. 2. A greater volume of data is required to precisely gauge the probabilities linked with each state as the number of states increases. 3. A BN featuring numerous states within a node might become less understandable. This approach is applied to the rest of the nodes as well.
Region	Eastern Asia, Europe, Middle east & North Africa, North America, Other	"Regions" experiencing fewer than three cyber-attacks are collectively categorized under the "other" state. The selection of regions is based on the frequency of cyber-attacks as well as the focus maritime entities in different areas of the world. For instance, Europe encompasses all territories surrounding the European continent, spanning both Western and Eastern Europe. While, Eastern Asia concentrates solely on this specific part of the continent, encompassing Southeast Asian countries due to the dense concentration of maritime entities in this region. This concept applies similarly to other regions across the globe.
Cyber threat origin	China, Iran, Nigeria, North Korea, Russia, Other, Unknown	It's important to clarify that identifying origin countries in cyber-attacks doesn't necessarily implicate the involvement of their states. The attribution is based on tracking the cyber-attack to a specific location. "Countries" involving fewer than three cyber-attacks are collectively categorized under the "other" state.
Consequence	Major, Minor	Consequences are categorized as "major" if they cause substantial disruption to the targeted entity's operations, resulting in significant physical and financial damage, as well as serious data theft and credential compromise. Conversely, attacks with less severe consequences are attributed to the "minor" category. To clarify this categorization, the NotPetya ransomware attack on Maersk, a major cyber-attack causing a $300 million loss, exemplifies significant consequences. Similarly, the hacking of India's Jawaharlal Nehru Port Container Terminal in February 2022, resulting in a five-day shutdown, underscores "major" repercussions. Conversely, less impactful incidents, either successfully thwarted or quickly recovered from, are labelled as "minor" cyber-attacks (Benmalek, 2024).
Year	2001–2023	–

results, 10 papers have been scrutinized for their relevance and content to extract the most significant SRIFs. Table 2 presents the selected literature along with their corresponding SRIFs.

2) Availability of factors in the database: It is essential to ensure that the selected SRIFs are well-represented in the database with minimal missing data, as factors with significant missing information can result in inaccurate or biased outcomes. Additionally, it is crucial to verify that the data related to these factors is consistently recorded and formatted. Inconsistent data can complicate the modelling process and diminish the reliability of the results. In this context, the SRIFs identified from the literature review were cross-referenced with the existing factors in the MCAD database to ensure a consistent selection process. For instance, factors such as scenario, property damage, prevention ability, and security risk level were identified in the literature review but were missing in the database. Consequently, these factors were excluded from further analysis.

3) Expert judgment and domain knowledge: Experts can offer insights that are not visible in data or literature alone, aiding in capturing the subtle complexities of the domain. In this study, we sought assistance from two experts with substantial knowledge and experience in this domain and requested their approval of the selected SRIFs.
4) Model testing and validation: By creating a preliminary TAN-based BN with the initially selected SRIFs and testing its performance, the least relevant factors can be identified. By eliminating these irrelevant factors and continuously refining the model through iterative adjustments based on performance metrics and the D-separation technique, the final SRIFs are selected. For example, we initially considered the factor "months of the year" to determine if it contributed to the occurrence of cyber threats. After running the model and testing this factor's influence on the target node, we found it to be irrelevant and ineffective. Therefore, it was excluded from the study.

For detailed information about the cyber SRIFs, their states, and descriptions, refer to Table 3.

3.3. Data-driven BN structure learning process

BN is an advanced graphical inference technique capable of modeling both subjective and objective data, taking into account the uncertainty associated with them. As a formal probabilistic approach, BN can also depict the causal relationships among random variables by employing conditional probabilities (Yang et al., 2018). In the construction of BN models, two primary approaches are typically employed. One of them relies on a data-driven method, where the connections between nodes are identified based on the inherent patterns within the data, often extracted through machine learning processes. The second approach is grounded solely in expert judgment, where the model is built based on the knowledge and experience of experts. In this method, it is the experts who determine the relationships between nodes, deciding which nodes are interconnected. In situations where a substantial amount of data is available, the data-driven approach tends to surpass the expert judgment approach. This is because employing empirical data helps minimize inherent biases associated with expert judgment.

This study aims to construct a BN structure by adopting the data-driven approach. This method seeks to capture various relationships, encompassing dependencies and interdependencies among different identified SRIFs. The literature presents diverse approaches that have been introduced and implemented for constructing BN using a data-driven approach. These approaches exhibit distinct strengths and weaknesses, influenced by factors such as the nature and volume of the data, the complexity of the network, the number of nodes and arrows, the extent of dependencies, and the validation methods employed, among others (Meng et al., 2022).

This paper employs the TAN Bayes algorithm, a data-driven approach among existing methods for constructing BN. TAN establishes a tree structure among features, with each node representing a feature and edges denoting dependencies between features. Typically, this tree is formed by designating the feature with the highest mutual information with the class variable as the node, followed by the addition of edges between features based on their mutual information with the class variable. TAN is designed to capture more realistic dependencies between features, offering greater flexibility compared to the conventional Naive Bayes model, while still maintaining computational efficiency. This algorithm is especially advantageous in scenarios where strong dependencies among features cannot be adequately addressed by the stringent independence assumption of Naive Bayes networks (NBN).

To elucidate this concept, a straightforward demonstration illustrating the disparity between NBN and TAN can be observed in Fig. 2. In NBN, attribute nodes are devoid of edges, thus capable of representing zero conditional dependencies. However, the assumption of conditional independence is overly rigid for real-world scenarios. When confronted with intricate attribute dependencies, this can lead to classification bias. For instance, in our scenario, the target node is defined as cyber threats with other attributes linked to it. Under the NBN framework, there are no interdependencies between the region and the year, thereby overlooking spatial-temporal considerations. TAN relaxes this independence assumption, extending NBN from a zero-dependence tree to a dependent maximum weighted spanning tree, purportedly enhancing classification performance compared to NBN.

To summarize the advantages of the TAN technique over alternative training methods, it can be analyzed from three distinct perspectives. Firstly, regarding interpretability, the tree structure in TAN offers a clear graphical representation of feature dependencies. This clarity facilitates the interpretation of model predictions and enhances the understanding of variable relationships. Secondly, in terms of robustness, TAN demonstrates greater resilience to irrelevant features compared to other techniques like traditional Naïve Bayes or general BN. Its tree structure aids in filtering out extraneous information, focusing instead on pertinent feature dependencies, thereby improving model performance and mitigating overfitting. Lastly, in terms of efficiency, despite its increased complexity relative to Naïve Bayes, TAN remains relatively quick to learn. This efficiency renders it suitable for datasets with moderate to large numbers of features, where fully learning the joint distribution could be computationally cumbersome, time-consuming, and costly (Jiang et al., 2012; Ren and Guo, 2023; Wu, 2018).

The conceptual foundation of this approach is detailed in the work of Friedman et al. (1997). To succinctly outline the fundamental steps in TAN learning, the process involves several key stages (Fan et al., 2020) which are demonstrated in Fig. 3. Its application in the context of maritime cybersecurity risk is detailed in the ensuing section.

Initially, the data is categorized into different classes known as SRIFs as represented in Table 3. Subsequently, data cleansing is performed, involving the removal of irrelevant entries and identification of missing data. Following this, the target node, representing the class variable for classification and serving as the starting point for tree modeling, is selected. In this case, the cyber threat is selected as the target node to understand how various factors contribute to the likelihood of different attacks occurring on various maritime targets. The qualitative structure of the TAN network is then established based on the mutual information between different nodes. Mutual information measures the statistical dependence between two variables. In the context of TAN, mutual information is used to quantify the relationship between each attribute and the class variable (target node). The mutual information between two variables X and Y is calculated as the reduction in uncertainty about X when the value of Y is known, and vice versa. It is commonly defined using entropy, a measure of uncertainty in a random variable. The mutual information between two discrete random variables X and Y is given by (Cover and Thomas, 2005):

$$I(X;Y) = \sum_{x \in X} \sum_{y \in Y} P(x,y) log \frac{P(x,y)}{P(x)P(y)} \quad (1)$$

where $P(x, y)$ is the joint probability mass function of X and Y, and $P(x)$

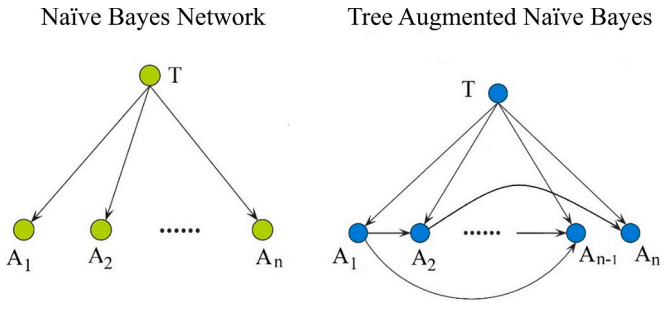


Fig. 2. The illustrative comparison between NBN and TAN structure learning.

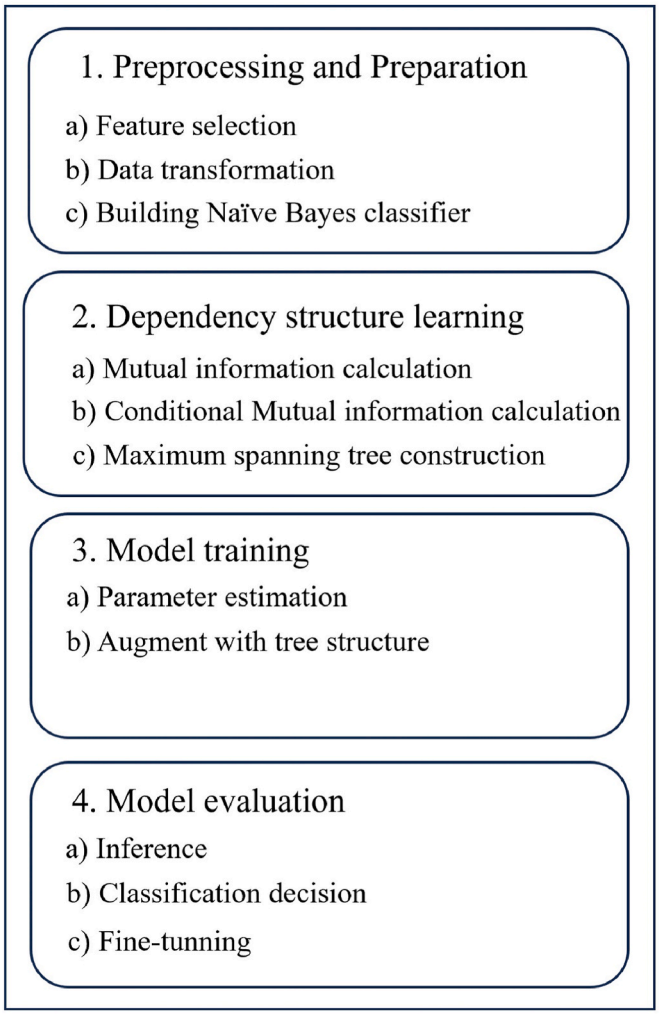


Fig. 3. TAN structure learning process.

and $P(y)$ are the marginal probability mass functions of X and Y, respectively. For instance, calculating mutual information between cyber threats and target entities reveals which types of entities are most frequently targeted by specific threats. This process is also carried out for all other nodes in the network concerning the target node.

Furthermore, with the class variable established, the relationships among various pairs of variables are discerned by computing conditional mutual information. This helps identify the most informative parent variable for each attribute in the network.

The conditional mutual information between two discrete random variables X and Y given Z is given by (Shannon and C.E. C. E., 1949):

$$I(X;Y/Z)=\sum_{x\in X}\sum_{y\in Y}\sum_{z\varepsilon Z}P(x,y,z)log\frac{P(x,y/z)}{P(x/z)P(y/z)} \quad (2)$$

As an example, the conditional mutual information between "origin countries" and "region" given the factor "year" reveals that cyber-attacks originating from certain countries are more prevalent in specific regions during particular years. This will help identify trends and hidden patterns among different contributing factors.

After obtaining the pairwise conditional mutual information, the maximum spanning tree algorithm is utilized to build a tree structure over the attributes in TAN. This typically involves employing heuristic algorithms like Prim's or Kruskal's algorithm, aiming to connect all attributes while maximizing the total weight of edges and minimizing network complexity (Cormen, 2009). Subsequent connections are made by calculating conditional mutual information among the remaining variables, ensuring that the tree structure reflects the most significant informational relationships. For instance, if the conditional mutual information between regions and target entities is high, an edge is added between them. This process continues for other pairs like victim countries and origin countries, ensuring each node is part of the spanning tree with cyber threats as the central node.

The parameter learning phase is executed to determine the conditional probability table for each node. Commonly employed methods for parameter learning and CPT acquisition in TAN encompass Maximum Likelihood Estimation, Bayesian Estimation, Expectation-Maximization, Markov Chain Monte Carlo, Structural EM, and others (Ji et al., 2015). The selection of a specific method hinges on factors such as the data's characteristics, computational resources, and assumptions regarding the data's underlying distribution. In this study, Bayesian estimation is chosen due to the completeness of the database, the absence of missing data, and the method's recognized accuracy and efficiency. The final stage encompasses model evaluation through three sub-steps: inference, classification decision, and fine-tuning. Inference calculates joint probabilities using the trained TAN model, guiding classification. Class labels are assigned based on the highest probability. Fine-tuning adjusts parameters to enhance predictive accuracy and robustness, ensuring optimal TAN model utilization in real-world scenarios.

3.4. Model validation process

Ensuring the reliability and effectiveness of the constructed model, accurately depicting the relationships between nodes, involves the implementation of various validation techniques. These techniques encompass comparative analysis, data splitting, metric analysis, and sensitivity analysis.

3.4.1. Comparative analysis and data splitting technique

The aim of comparative analysis in BN validation is to ensure the competitiveness and efficacy of the model against the established methods in the field. This boosts confidence in its validity by assessing its performance against other relevant models. Various methods can be used; for example, comparing it with conventional approaches or widely used algorithms in cybersecurity. In this study, due to limited quantitative methodologies for maritime cyber-attacks, predicted probabilities are contrasted with statistical counterparts, aiming for consistency and reliability. In another approach for validation purposes, the data-splitting technique, or train-test split, has been implemented, which involves dividing a dataset into training and testing subsets. This allows assessment of how well a model generalizes to new data (Joseph, 2022). Typically, 80% of the data is used for training, enabling the model to learn relationships and structure. The remaining 20% is reserved for testing, evaluating the model's performance on unseen data. Accurate predictions on this set indicate model validity (Li et al., 2024a,b). Splitting data ensures robust evaluation and enhances confidence in the model's ability to perform effectively on real-world data.

3.4.2. Metric analysis

An alternative method worth considering for validating BN models is the use of metric analysis. This approach employs diverse quantitative measures to assess the alignment between the constructed BN model and real-world data. It offers a thorough evaluation of the model's predictive abilities and its effectiveness in capturing patterns within the data. In this study, four widely recognized metrics have been chosen for this purpose, namely Precision, Recall, F-measure, and Specificity. These metrics are computed using the derived confusion matrix, which encompasses predictions categorized as true positives, true negatives, false positives, and false negatives (Hu et al., 2016). The confusion matrix serves as a comprehensive summary of the BN model's predictions, juxtaposing them against the actual class labels in the dataset. In the matrix, the rows denote the actual classes, while the columns represent the predicted classes. The term "confusion" matrix is apt as it illustrates

where the model might experience confusion or make errors in its predictions. Primarily, the key consideration is the overall accuracy of the model, which is directly derived from the confusion matrix. This metric signifies the total percentage of correct predictions made by the model. Put simply, it calculates the ratio of instances that were correctly predicted to the total number of instances. An accuracy rate exceeding 90 percent is generally regarded as indicative of a reliable model. The rest of the measures are described in Table 4 with their corresponding formulas (Powers and Powers, 2011).

3.4.3. Sensitivity analysis

Undoubtedly, sensitivity analysis is widely recognized as a crucial technique for validating developed models, and BN models are no exception. Sensitivity analysis involves monitoring the output as changes are introduced to the input. In this scenario, slight adjustments are made to the values assigned to the variables within the BN, and the model's outcomes are examined to ensure they respond accordingly. Additionally, this analysis aids in identifying the most significant variables that exert the greatest influence on the target node. In this paper, sensitivity analysis is conducted through four primary approaches, which include mutual information, joint probability, True Risk Influence (TRI) (Alyami et al., 2019), and variation testing.

Within the realm of BN, mutual information, as its name suggests, is a metric that measures the level of dependence or information shared between two random variables. It measures the extent of interdependence or shared information between two specific variables in the network. A greater mutual information value signifies a more robust association, implying that alterations in the values of one variable are likely to exert a more significant influence on the other. This information proves valuable for comprehending the consequences of varying inputs on the overall behavior of the BN.

In order to pinpoint the crucial variables in a BN that exert the most significant influence on the target node, this paper adopts the TRI technique proposed by Alyami et al. (2019). TRI is defined as the average of High-Risk Influence (HRI) and Low-Risk Influence (LRI) values. The computation of these values involves specific procedures: HRI is determined by elevating the probability of the state of a random SRIF with the most substantial impact on the target node, identified through joint probability, and subsequently reducing the original value of the specific state of the target node. LRI follows a similar process, but the variable chosen has the least substantial impact on the target node. This approach is based on the rationale that conventional sensitivity analysis, wherein different values are assigned to the states of the nodes under investigation while keeping the states of other nodes constant, is generally suitable for nodes with only two states. In the case of nodes with multiple states, changing values in this manner becomes challenging. Consequently, identifying only two states with the highest and lowest values among others appears more pragmatic for applying the traditional method of sensitivity analysis.

The final method utilized for sensitivity analysis in this paper is referred to as minor variation testing. This straightforward approach adheres to two fundamental principles (Zhang et al., 2013):

Axiom A: A marginal increase or decrease in the prior probabilities of each tested node should result in a proportional increase or decrease in the posterior probability of the target node.

Axiom B: The overall impact of incorporating probability variations from the evidence should be at least as substantial as the impact from a subset of the evidence.

In accordance with these axioms and meeting their criteria, a minor alteration, not exceeding the value of the smallest state among all SRIFs, is systematically applied to different nodes. These nodes are prioritized based on mutual information results. The process is iteratively performed for all nodes while preserving previous outcomes. The gradual shifts in results signify the cumulative impact of probability variations in the input.

Table 4
The validation metrics.

Measure	Formula	Description
Precision	$\frac{\text{True positive}}{\text{True positive} + \text{False positive}}$	The accuracy of positive predictions, expressing the percentage of true positives among all instances that the model has predicted as positive.
Recall	$\frac{\text{True positive}}{\text{True positive} + \text{False negative}}$	Assesses the model's ability to capture all relevant instances by calculating the ratio of true positives to the sum of all actual positive instances.
F-measure	$2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$	Represents a balance between precision and recall, providing a single metric that considers both false positives and false negatives.
Specificity	$\frac{\text{True negative}}{\text{True negative} + \text{False positive}}$	Measures the ability of the model to correctly identify negative instances by calculating the ratio of true negatives to the sum of true negatives and false positives.

4. Results

4.1. TAN-based BN modeling construction

Employing the identified SRIFs outlined in Table 3 and designating the cyber threats as the target node, the TAN model for maritime cybersecurity is constructed. This modeling process was carried out using Netica software (Netica, 2019), as illustrated in Fig. 4. The resulting model adeptly captures and signifies the probabilistic dependencies among various variables, employing a specific structure conducive to streamlined computations. Following the model's establishment, it undergoes a data-driven procedure wherein the diagnostic and prognostic capabilities of the model are activated based on the feeding of prior data, enhancing its practical utility.

4.2. Model validation

Using the concepts and validation methodologies described in Section 3.4, the constructed BN model for cyber threats undergoes validation to assess its accuracy in both diagnostic and prognostic capabilities. Table 5 presents a comparison between the results of statistical analysis and the TAN model, revealing a substantial level of agreement.

The findings indicate that ransomware emerges as the most prevalent form of cyber-attacks in stationary maritime infrastructures, followed by hacking, malware, phishing, and DDOS. It's important to highlight that all the recorded DDOS attacks occurred within seaports. In the case of vessels, the two most frequent cyber-attacks are spoofing and jamming, respectively. Regarding cyber threats against vessels, certain regions worldwide are more susceptible than others. Jamming incidents are frequently observed in Eastern Asia, while spoofing tends to be more prevalent in the seas around Europe and Northern America. In terms of time, the recent years, specifically over the past five years, have witnessed a notable increase in cyber-attacks, reaching a peak in 2020 and 2021. This trend suggests a continuous upward trajectory. These initial findings suggest that BN outperforms statistical analysis. BN demonstrates the ability to identify causal relationships and the interdependence of various variables, showcasing its superiority in this context. Another validation method utilized in this phase is the D-separation technique. D-separation (or Directed Separation) is a key concept in BN modeling, used to determine conditional independence between nodes. It helps in assessing whether two variables are independent given certain evidence, making it essential for reasoning within the network (Yu et al., 2021). After the BN is initially constructed, D-separation is applied to examine correlations between any two nodes in the network. For instance, when the "cyber threat" node is observed, the nodes "Target" and "Region" become independent, meaning they are

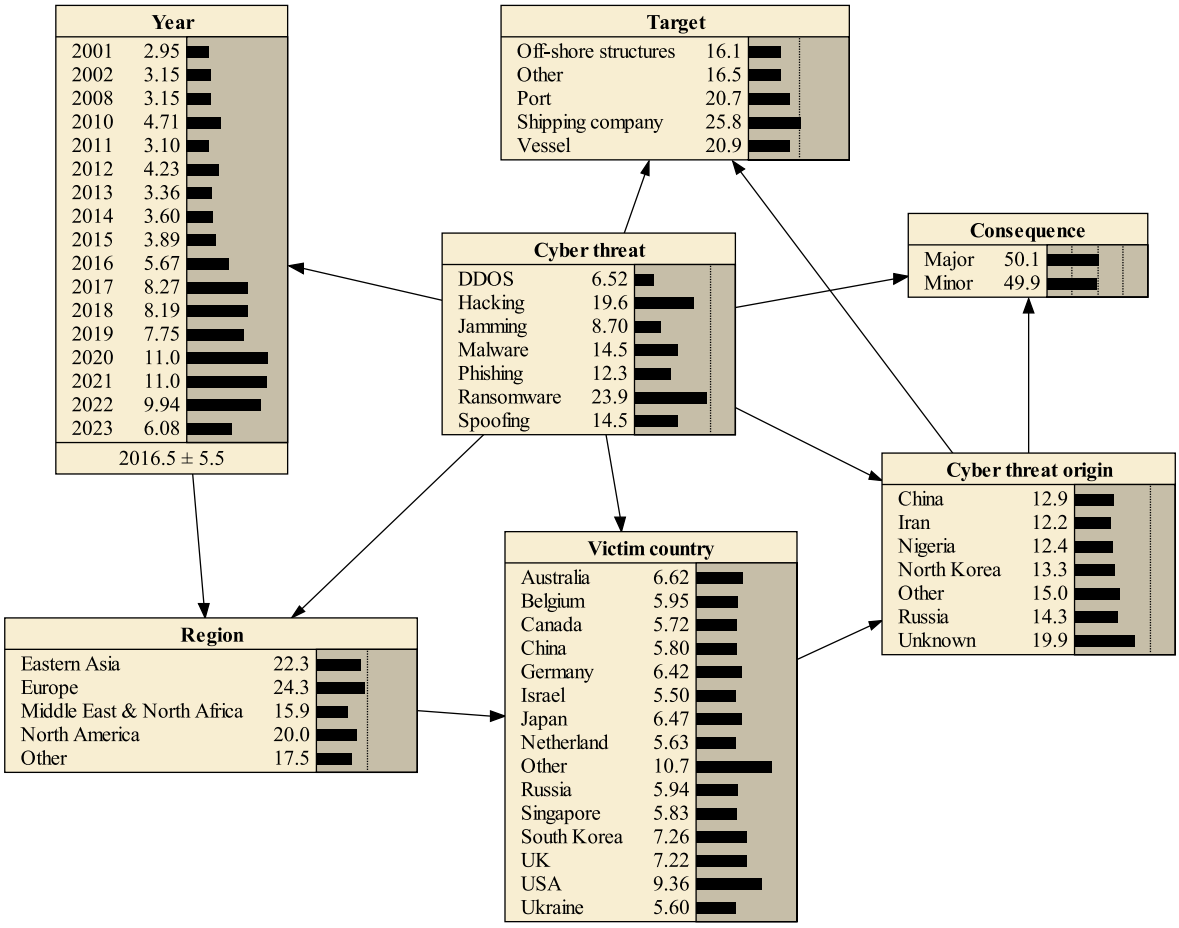


Fig. 4. TAN-based BN model of cyber attacks.

Table 5
Comparative analysis of historical and TAN results.

Attack type	Historical data (%)	TAN results (%)	Accuracy (%)
DDOS	6.80	6.52	95.8
Hacking	19.1	19.6	97.4
Jamming	8.70	8.70	100
Malware	14.8	14.5	98
Phishing	11.7	12.3	95.1
Ransomware	24.1	23.9	99.2
Spoofing	14.8	14.5	98

D-separated and conditionally independent. Conducting similar analyses across other nodes and connections helps to validate the BN structure, ensuring its rationality.

To assess the prognostic capability of the developed model, a data splitting process is employed by reserving 20 percent of the collected data for testing. The model is trained using the remaining 80 percent of the data. The resulting confusion matrix, as depicted in Table 6, reveals an overall accuracy exceeding 93 percent, with a perfect predictability rate of 100 percent for the majority of the target states. This indicates a high level of success in the model's ability to make accurate predictions and underscores its reliability for prognostic purposes.

After obtaining the accuracy rate from the confusion matrix, an additional metric is utilized to validate the model's reliability, known as the Kappa coefficient, often referred to as Cohen's Kappa (Cohen, 1960). This statistical measure evaluates the degree of agreement between two raters or observers when categorizing or classifying items. In the context of this paper, the aim is to quantify the agreement between predicted and actual results. By applying the Kappa coefficient formula and incorporating relevant values, such as the expected proportion of agreement and the observed proportion of agreement derived from the confusion matrix (representing overall accuracy), the calculated Kappa coefficient is 0.92. The result suggests a remarkable degree of consistency in the model, as per Landis and Koch (1977), where a coefficient exceeding 0.8 is deemed ideal. This underscores a level of agreement that far exceeds what might be expected through random chance.

In line with the information provided in the validation section, Fig. 5 displays diverse performance metrics for each cyber-attack based on an analysis of the confusion matrix. Notably, the model's precision is remarkably high, reaching 100% for the majority of cyber-attacks and maintaining satisfactory values above 75% for the rest. Concerning Recall, hacking and malware exhibit values of 66.6% and 75%, respectively, while other types of attacks achieve a perfect 100%. The F-measure, a metric that harmonizes precision and recall, surpasses 75% across all categories, with the majority scoring above 90%, indicating a well-balanced assessment of the model's performance. As previously mentioned, a higher specificity contributes to enhanced model robustness. Specifically, DDoS, hacking, jamming, and phishing showcase a specificity of 100%, while malware, ransomware, and spoofing, though around 96%, still indicate substantial robustness. An analysis of these performance metrics highlights the notable reliability and robustness exhibited by the developed model.

During the next phase of the validation process, the strength of the relationship between cyber threats and other SRIFs is assessed by measuring mutual information, as detailed in Table 7. Significantly, the analysis indicates that the factor of "year" emerges as the most impactful, far surpassing the influence of "target" and the "countries falling victim" to cyber threats. This underscores the paramount importance of temporal considerations, the type of targets and the readiness of cyber

Table 6
Confusion matrix of predicted results.

		Actual							Actual total	Accuracy rate (%)
		DDOS	Hacking	Jamming	Malware	Phishing	Ransomware	Spoofing		
Predicted	DDOS	3	0	0	0	0	0	0	3	100
	Hacking	0	4	0	1	0	1	0	6	66.6
	Jamming	0	0	3	0	0	0	0	3	100
	Malware	0	0	0	3	0	0	1	4	75.0
	Phishing	0	0	0	0	3	0	0	3	100
	Ransomware	0	0	0	0	0	7	0	7	100
	Spoofing	0	0	0	0	0	0	5	5	100
	Total	3	4	3	4	3	8	6	31	93.3

defense abilities of countries in comprehending and addressing cybersecurity challenges, with a notable distinction in the significance of these factors.

Based on the details outlined in Section 3.4, the joint probability of the target node (referred to as cyber threats) and other relevant variables across different nodes is computed and displayed in Table 8. Altering the values of various states in nodes induces corresponding changes in the states of the target node. The extent of these variations is contingent upon the significance of the states influencing the target node. To facilitate clarity and highlight the most and least influential factors, bold formatting is applied to the highest and lowest values for both types of terrorist attacks. The joint probability analysis yields valuable insights: seaports are predominantly targeted by DDOS attacks, whereas ransomware incidents are more common in the context of shipping companies. Spoofing, on the other hand, tends to disrupt the normal operation of vessels. From a temporal perspective, the early years saw DDOS as the dominant cyber-attack type on stationary infrastructures like seaports; however, in recent years, ransomware has gained traction among attackers. This trend extends to vessels, which were previously disrupted by jamming but now face spoofing, considered a more sophisticated version of jamming. Spatially, European and North American seaports are more targeted by ransomware, while phishing and malware emerge as typical cyber threats for Asian targets. Further insights on this matter will be expounded upon in Section 5.

Taking into account the noteworthy findings highlighted in bold from the joint probability analysis, the TRI for all SRIFs is computed using the procedure outlined in Section 3.4, and the outcomes are presented in Table 9. The results underscore that the factor "year" emerges as the most influential, significantly impacting the target node. In comparison to other SRIFs, "year" obtains the highest TRI value by a substantial margin for all types of cyber-attacks. Following, the victim country stands out as the second most important variable, with "target" trailing closely. The remaining SRIFs can be ranked in the following order: region, cyber threat origin, and, finally, consequence. These findings shed light on the relative importance of these factors in assessing cyber threats in the context of the maritime industry.

Table 7
Mutual information between cyber threats and other SRIFs.

Node	Mutual information	Percentage (%)	Variance of belief
Cyber threat	2.69722	100	0.7011338
Year	0.24606	9.12	0.0165646
Target	0.06310	2.34	0.0028549
Victim country	0.03683	1.37	0.0016443
Consequence	0.03446	1.28	0.0012589
Region	0.02861	1.06	0.0012553
Cyber threat origin	0.01744	0.646	0.0007828

In the final stage of the validation process, the developed BN model undergoes sensitivity testing. Following the ranking obtained through mutual information, each variable is systematically adjusted, starting from the least important to the most crucial, with a 3 percent incremental change, and the resulting impact on the target node states is observed. Fig. 6 illustrates the gradual increase in the elements of the bar chart for all types of cyber threats, clearly indicating that the model responds to the changes in a discernible manner. This sensitivity testing further validates the robustness and adaptability of the BN model in capturing the dynamics of the interrelated variables and their influence on the target states.

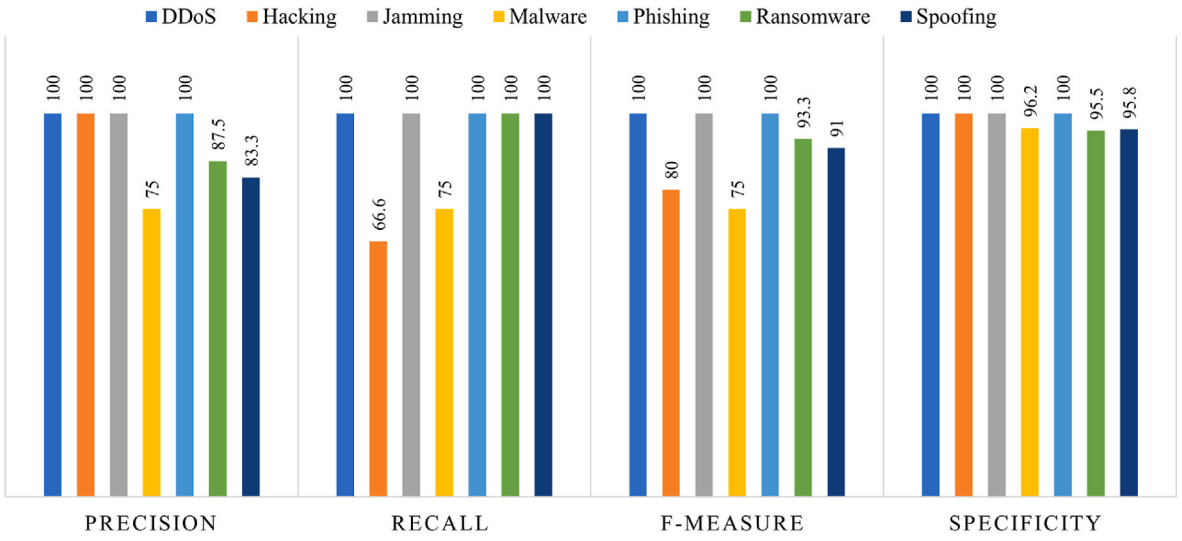


Fig. 5. The performance metrics for different cyber-attacks.

Table 8
The joint probability.

	DDOS	Hacking	Jamming	Malware	Phishing	Ransomware	Spoofing
Target							
Off-shore structure	6.76	20.6	8.74	14.9	14.1	22.3	12.5
Other	6.58	18.0	8.51	**16.3**	13.5	24.9	12.2
Port	**10.5**	**22.6**	8.22	**11.8**	8.68	28.5	9.75
Shipping company	**4.22**	21.0	**5.46**	16.3	**16.4**	**28.7**	**7.84**
Vessel	5.21	**15.2**	**13.3**	13.2	**8.60**	**13.9**	**30.7**
Year							
2001	**17.7**	15.4	10.5	13.6	12.6	16.5	13.6
2002	8.29	28.9	9.87	12.8	11.9	15.5	12.8
2008	8.29	28.9	9.87	12.8	11.9	15.5	12.8
2010	5.54	9.67	6.60	**51.3**	7.93	10.4	8.55
2011	8.43	14.7	10.0	26.0	12.1	15.8	13.0
2012	6.16	21.5	14.7	19.0	17.6	11.5	9.51
2013	15.5	13.6	9.25	24.0	11.1	14.5	12.0
2014	7.24	**37.9**	8.62	11.2	10.4	13.5	11.2
2015	6.70	23.4	7.97	10.3	28.8	12.5	10.3
2016	9.19	16.0	**38.3**	7.09	6.58	8.60	14.2
2017	6.31	33.0	3.75	9.73	**31.6**	**5.90**	9.73
2018	6.37	16.7	15.2	14.8	4.56	17.9	24.6
2019	3.37	**5.87**	4.01	15.6	9.63	25.2	**36.4**
2020	**2.37**	20.7	**2.82**	**3.66**	**3.39**	**48.8**	18.3
2021	2.38	16.6	2.84	25.7	10.2	31.2	11.0
2022	5.25	18.3	6.25	4.05	18.8	39.3	8.10
2023	12.9	22.5	5.11	6.62	6.14	40.2	**6.62**
Victim country							
Australia	5.93	23.3	7.52	11.4	10.1	30.2	11.5
Belgium	6.60	16.3	8.37	15.2	11.3	26.7	15.5
Canada	**9.64**	20.3	8.69	13.2	11.7	23.1	13.3
China	6.77	16.7	8.58	13.0	11.6	18.8	**24.5**
Germany	6.11	21.3	7.75	11.8	12.6	28.6	11.9
Israel	8.57	21.0	10.8	13.7	12.2	19.8	13.8
Japan	6.06	**24.0**	7.68	20.2	10.4	19.9	11.7
Netherland	8.39	17.2	8.84	13.4	11.9	23.8	16.4
Other	**3.67**	**16.1**	7.36	17.6	**16.8**	28.3	**10.2**
Russia	6.61	16.3	8.38	15.3	11.3	18.4	23.8
Singapore	6.73	20.0	8.53	13.0	16.6	22.1	13.0
South Korea	5.41	18.7	**18.5**	**20.5**	11.3	**15.0**	10.5
UK	6.54	21.7	6.89	10.5	15.1	22.0	17.3
Ukraine	7.01	17.3	8.88	18.8	12.0	19.5	16.5
USA	6.74	22.8	**5.32**	**9.58**	**8.51**	**34.0**	13.1
Cyber threat origin							
China	6.68	19.6	8.55	16.5	14.4	19.8	14.4
Iran	**7.54**	19.3	9.02	14.1	12.3	22.5	15.2
Nigeria	6.96	17.9	8.90	13.9	**17.7**	20.6	13.5
North Korea	6.47	18.9	**13.3**	**16.9**	11.3	**19.2**	13.9
Other	6.15	21.2	7.36	14.0	10.8	28.1	12.4
Russia	6.87	**15.5**	7.69	14.6	**10.5**	24.3	**20.7**
Unknown	**5.58**	**22.9**	**7.10**	**12.5**	10.8	**29.3**	**11.9**
Consequences							
Major	**5.03**	**20.4**	**9.11**	**16.4**	**12.7**	**28.6**	**7.84**
Minor	**8.02**	**18.7**	**8.28**	**12.6**	**11.9**	**19.2**	**21.2**
Region							
Eastern Asia	**5.18**	18.4	**11.9**	**20.6**	**14.0**	**15.1**	14.8
Europe	5.58	**16.4**	**6.70**	11.7	12.6	**29.6**	**17.5**
Middle east & North Africa	**7.99**	21.3	10.6	16.3	13.1	17.6	13.1
North America	7.93	21.3	6.82	**11.2**	**9.95**	28.9	13.9
Other	6.60	**21.8**	7.82	12.8	11.8	27.2	**11.9**

Table 9
TRI of SRIF for different cyber threats.

	DDOS	Hacking	Jamming	Malware	Phishing	Ransomware	Spoofing	Average
Year	7.67	16.02	17.74	23.82	14.11	21.45	14.89	**16.53**
Victim country	2.99	3.95	6.59	5.46	4.15	9.50	7.15	**5.68**
Target	3.14	3.70	3.92	2.25	3.90	7.40	11.43	**5.11**
Region	1.41	2.70	2.60	4.70	2.03	7.25	2.80	**3.36**
Cyber threat origin	0.98	3.70	3.10	2.20	3.60	5.05	4.40	**3.29**
Consequence	1.50	0.85	0.42	1.90	0.40	4.70	6.70	**2.35**

5. Discussions, implications, and future research directions

5.1. Discussions

5.1.1. Different types of cyber-attacks

Examining the compiled database obtained from MCAD and utilizing the BN model built from this information, seven distinct cyber threats were discerned within the maritime sector. These include DDOS, hacking, jamming, malware, phishing, ransomware, and spoofing. Notably, ransomware stands out as the most prevalent threat, accounting for nearly 25% of all documented incidents, followed by hacking, which comprises almost one-fifth of the total attacks. Through the utilization of the model and scenario analysis, valuable information and insights are acquired. For instance, by elevating the probability of ransomware to 100%, an effort is made to discern the primary contributing factors influencing the selected state of the target node. Illustrated in Fig. 7, the probabilities associated with various states of other SRIFs undergo changes, signaling specific insights. Concerning the target, ransomware exhibits a preference for targeting shipping companies and seaports. This preference can be rationalized by the fact that ransomware attackers commonly demand cryptocurrency payments to restore access to compromised systems, compelling companies and seaports to potentially pay the ransom to mitigate downtime and operational disruptions. In terms of time, an examination of the past four years reveals a notable surge in ransomware incidents, with the peak occurring in 2020. Analyzing the geographical distribution of these attacks, Europe emerges as the primary target, closely followed by North America. Among the specific nations affected, the United States, Australia, and Germany stand out as the top three victim countries experiencing ransomware incidents. Notably, a significant majority of these cyber-attacks fall into the category of major incidents, underscoring the severity of their consequences. This temporal and geographical analysis highlights the alarming trend of ransomware activity over the specified period and emphasizes the global impact of these malicious incidents.

Applying a methodology similar to the one employed for ransomware, valuable insights can be derived concerning other cyber threats. Particularly noteworthy are DDoS attacks, renowned for their disruptive impact, all meticulously documented within the realm of seaports, causing disruptions to their regular operations. Fig. 8 represents the corresponding values for different SRIFs when the DDoS cyber-attack is set as 100 percent. Notably, the majority of these attacks have been directed at U.S. seaports, with a discernible origin traced back to Russia. Examining the timeline, a significant surge in DDoS attacks has been observed in 2023, underscoring the critical nature of the situation during this period.

The patterns observed in hacking, malware, and phishing incidents exhibit striking similarities concerning their targets and consequences. However, when viewed through a temporal lens, hacking records appear to be distributed relatively evenly over the past five years. In contrast, malware incidents reached their peak in 2019, and phishing incidents were most pronounced in 2017. In terms of spatial distribution, Eastern Asia emerges as a focal point for malware and phishing activities, collectively accounting for one-third and one-fourth of all incidents worldwide, respectively. This geographical concentration underscores the significance of Eastern Asia in the prevalence of these cyber threats on a global scale.

When considering cyber-attacks such as jamming and spoofing that specifically target vessels, two prominent countries, namely North Korea and Russia, have been identified as leading actors in deploying these tactics against maritime targets. The prevalence of jamming incidents has notably affected the majority of South Korean vessels, consequently establishing Eastern Asia as the region with the highest frequency of jamming events from a geographical standpoint. Spoofing, characterized as a more sophisticated form of jamming, has witnessed prevalent usage, particularly in European seas, over the past five years. Russia, in particular, is acknowledged as a trailblazer in employing spoofing attacks against vessels in these maritime regions.

5.1.2. Top cyber SRIFs

Taking into account the findings presented in Table 9, the top cyber SRIFs, ranked according to their TRI values, are identified as the year, victim country, and target. Identifying the "year" as the foremost influential factor in cyber SRIFs highlights the importance of considering the temporal dimension when assessing cyber threat trends in the maritime domain. Over the last five years, nearly 60% of recorded cyber-attacks have exhibited a significant surge, peaking in 2020 and 2021. This pattern indicates a consistent upward trend. In contrast, attacks from the years preceding 2016 contribute only 15% to the overall recorded incidents. Given this pattern, the primary explanation that arises is the

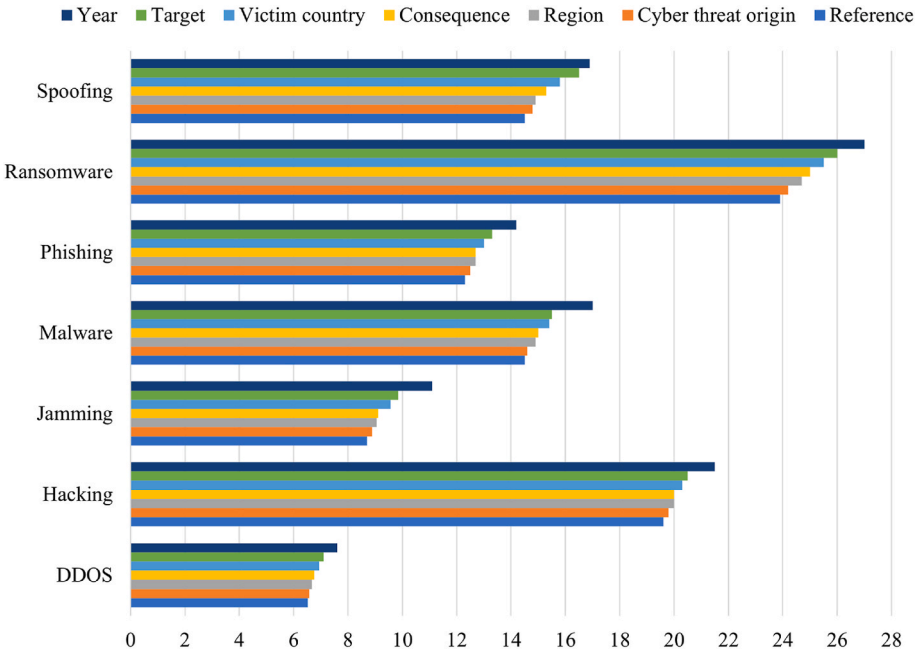


Fig. 6. Sensitivity analysis of BN model.

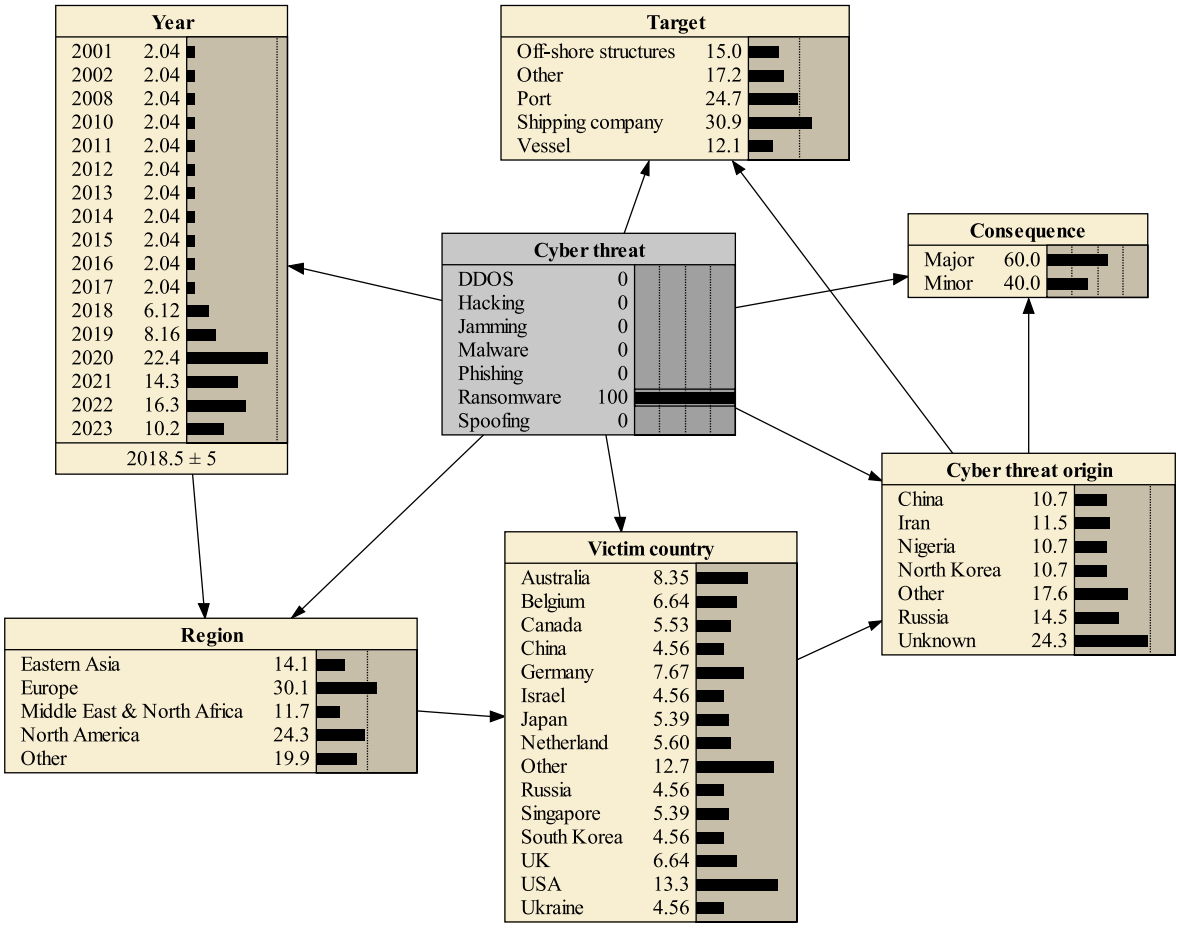


Fig. 7. Ransomware cyber-attack scenario.

technological advancement, the increasing digitization of systems, and the substantial reliance of the maritime sector on network-based communications and applications. The evolution in technology broadens the potential targets and expands the attack surface for cybercriminals to take advantage of vulnerabilities. Emerging digital systems may not possess sufficient cybersecurity protections when compared to traditional analog or manual operations. Another factor to consider is the evolving tactics, techniques, and procedures employed by cyber-attackers over time. They continually refine their approaches to circumvent security measures, with methods becoming more sophisticated as defenses strengthen. Additionally, there is an increased collaboration among cybercriminals, who have established their own networks to exchange information, knowledge, and experience, facilitating the execution of cyberattacks. Furthermore, the accessibility and ease of use of hacking tools online have reduced the resources required for cyberattacks, enabling even less skilled attackers to target maritime infrastructure. From a different perspective, the response time of regulations and the industry lags behind the pace of evolving cyber threats. The emergence of new cyber threats often precedes the establishment of new regulations or industry best practices to address them, providing attackers with a window of opportunity. To further analyze the dependence of specific years and types of cyberattacks, Fig. 9 illustrates the distribution of various cyberattacks in the maritime industry from 2016 to 2023. The evolving trend in maritime cyber threats is evident, with different attack types peaking at different times. Significant increases in specific attack types underscore the dynamic nature of these threats and highlight the need for adaptive and robust cybersecurity measures in the maritime industry. In 2016, jamming attacks reached an extremely high percentage, nearly 70%, significantly higher than any other type of attack that year. This suggests a specific vulnerability or focus on jamming attacks in the maritime sector during this period. Conversely, the more sophisticated version of jamming, known as spoofing, shows an increasing trend in subsequent years, reaching its peak in 2021. In 2017, phishing incidents saw a substantial increase, accounting for nearly 50% of the reported cases. This highlights a shift or escalation in targeting individuals within the maritime industry during this year. However, the number of phishing incidents began to decrease in the following years, which can be attributed to improved cybersecurity training and increased awareness of these types of threats among individuals in the industry. As seen over the past few years, ransomware attacks have gained popularity among cyber attackers, spiking dramatically in 2020 and accounting for almost 60% of all cyber incidents. Despite moderate fluctuations, ransomware has continued to be the most frequent cyber threat up to the present. This marks ransomware as the dominant threat in the maritime sector, likely reflecting broader global trends in cybercrime where ransomware has become increasingly prevalent. For the other types of cyber threats, the trend has followed an oscillating pattern over the years, indicating a consistent underlying threat. Overall, scrutinizing the temporal dimension of cyber threats highlights the importance of historical data in understanding and predicting future threats. This emphasizes the necessity of continuous monitoring and regular updates to cybersecurity strategies to effectively address the most pressing vulnerabilities. Furthermore, “year” has been an important influetial factor in other maritime security studies such as maritime terrorism risk analysis (Mohsendokht et al., 2024) and cargo theft from freight supply chains (Liang et al., 2022).

The recognition of “country” as the second most significant SRIF underscores the crucial role of national and governmental readiness in dealing with cyber-attacks. Unlike physical terrorist attacks, which are often prevalent in developing countries or regions facing political or economic instability, cyber-attacks are predominantly observed in developed nations, with the USA having the highest number of recorded incidents.

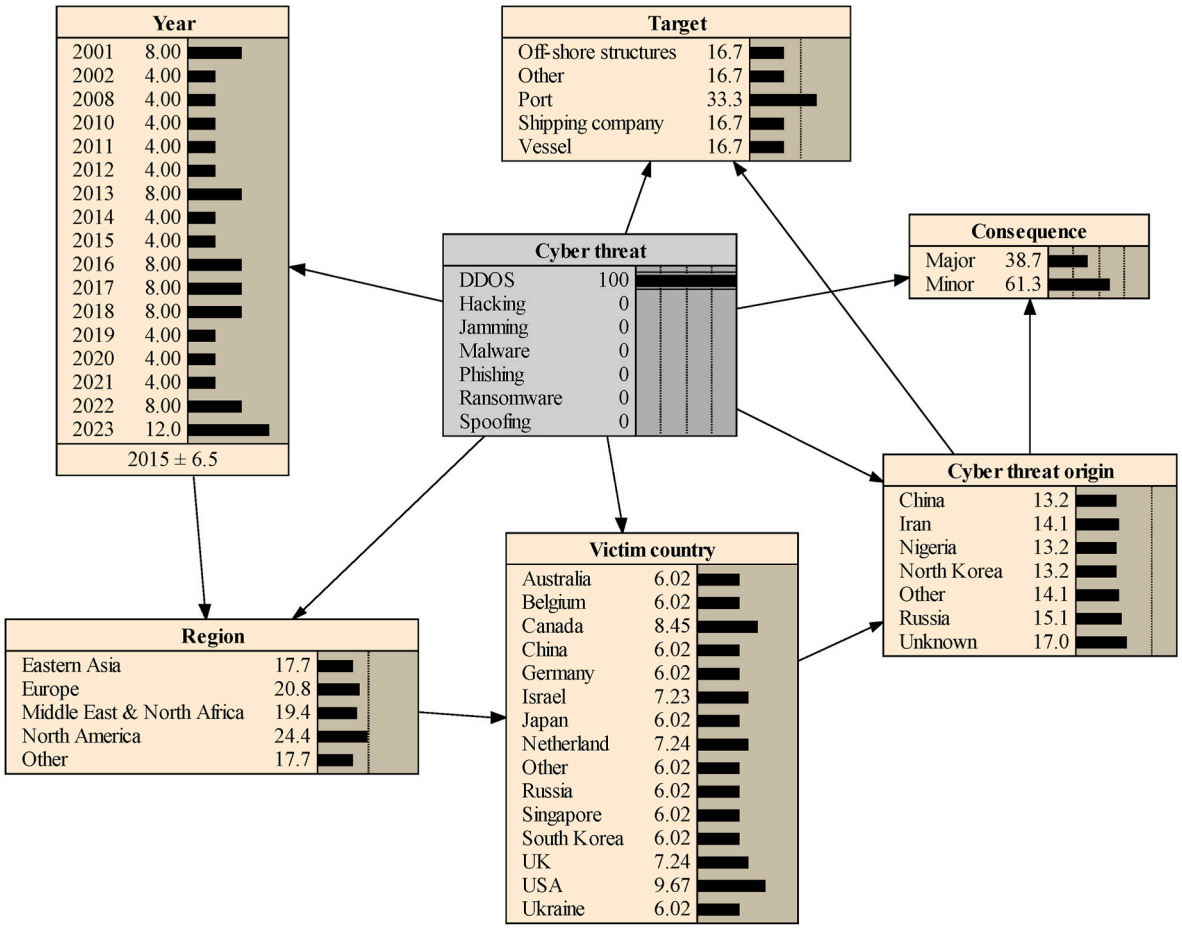


Fig. 8. DDoS cyber-attack scenario.

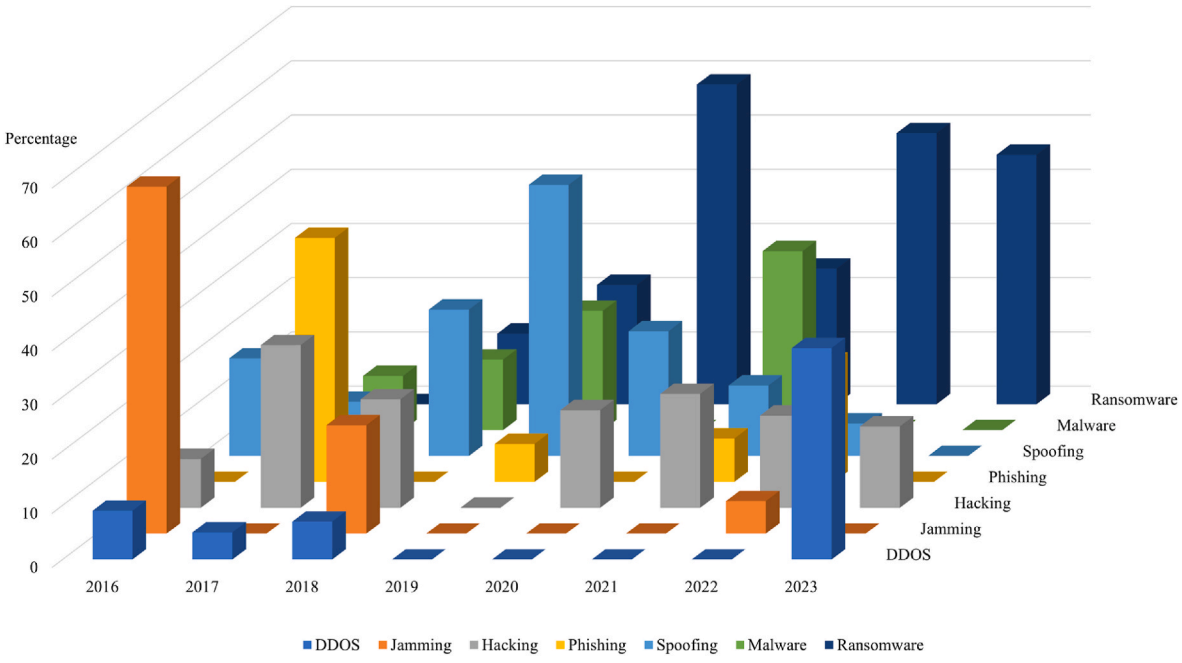


Fig. 9. The distribution of cyberattacks over the past 8 years.

This observation can be understood from different angles. Firstly, it relates to the widespread use of advanced, high-tech digital systems across various sectors of the maritime industry, such as seaports, shipping companies, offshore structures, and transportation vessels. These technological advancements are typically more prevalent in developed countries, rendering them more susceptible to cyber-attacks. Secondly, the nature of cyber-attacks is characterized by the absence of geographical constraints. This means that an attacker from any part of the world can pose a threat to the infrastructure of a victim country, regardless of the distance between them. Thirdly, when considering ransomware as the most prevalent form of cyber-attacks, the wealth of developed countries renders them attractive targets for such incidents, serving as a means of fundraising for cybercriminals. The financial resources and economic strength of these developed nations make them tempting targets for malicious actors seeking monetary gains through cyber extortion. This highlights the need for advanced preparedness measures at a national and governmental level to address cyber threats effectively.

The third cyber SRIF is linked to the nature of the target. Through the data-driven approach, five distinct maritime targets have been identified as susceptible to cyber-attacks, including ports, shipping companies, vessels, off-shore structures and others. Among these, shipping companies, encompassing various businesses involved in the global supply chain, emerge as the primary focus of cyber threats, followed by ports as the main hub for maritime transportation. This heightened susceptibility can be attributed to several key factors. Firstly, these entities are pivotal strategic assets that hold a central role in the global supply chain, rendering them attractive targets for cyber attackers aiming to disrupt international trade and commerce. Secondly, the complex operations within shipping companies and ports, involving a multitude of stakeholders, diverse cargo types, and complex logistics, create an environment with increased opportunities for cyber vulnerabilities. Additionally, the extensive scale of operations in shipping and port activities contributes to a broader attack surface, making them more vulnerable to cyber threats compared to smaller maritime structures. Furthermore, the nature of sensitive information handled by shipping companies and ports, encompassing details about cargo, routes, and logistics, adds to their attractiveness as targets. This valuable data can be exploited by cyber attackers for financial gain, operational disruption, or ransom demands, a trend substantiated by the prevalence of frequent ransomware cyber-attacks in this sector. This emphasizes the urgent need for stakeholders, governments, and decision-makers to redirect their focus towards the vulnerable sectors of the maritime industry and allocate sufficient resources to fortify them against potential cyber-attacks. It is imperative to implement proactive measures and robust cybersecurity strategies to safeguard the critical functions of shipping companies and ports, thereby ensuring the resilience and security of the global supply chain.

5.1.3. Comparative examination of research findings

In this section, a succinct comparison between the current research outcomes and those of various relevant studies in the domain is conducted. The aim is to underscore the commonalities, distinctions, and comprehensiveness of each study, thereby accentuating the significance of our work. For this purpose, seven recent journal papers centered on cybersecurity risk assessment are selected. These papers have developed quantitative frameworks that yield comparable result categories. The categories encompass various aspects, including distinct cyber-attack types, data classifications, diverse types of SRIFs, targets, application domains, prioritization of cybersecurity factors, analysis of SRIF interdependencies, and implications within the domain, as delineated in Table 10. As evident, the present paper offers a more comprehensive perspective on the aforementioned categories, providing a more realistic depiction of results attributed to its reliance on objective data for analysis.

5.2. Implications

The implications derived from the study's findings are discussed across technical and organizational perspectives.

From a technical standpoint, considering the widespread occurrence of ransomware, it is crucial for maritime stakeholders, particularly shipping companies and seaports, to prioritize robust cybersecurity measures to safeguard against ransomware attacks. To achieve this, effective measures include implementing routine backups, utilizing network segmentation, ensuring offline storage, and providing employee training. In the context of DDoS attacks, investments in scalable infrastructure, anomaly detection systems, and collaboration with internet service providers can help mitigate their impact (De Neira et al., 2023). Generally, maintaining up-to-date software and deploying real-time threat monitoring systems utilizing AI for detecting unusual network activities, indicative of a cyber-attack, enables prompt action and enhances the defensive capabilities of the target (Boudehenn et al., 2021; Caprolu et al., 2020; Freire et al., 2022; Laso, 2022). In dealing with cyber threats such as hacking, phishing, and malware, mitigating risks involves conducting regular security audits and employing robust security measures like strong passwords and multi-factor authentication. It is essential for shipping companies and ports to stay vigilant by keeping anti-virus software up-to-date and offering training on identifying phishing attempts. Additionally, implementing mechanisms such as email filtering and validation can enhance the ability to identify and block phishing attempts (BIMCO, 2018). To safeguard against the risks of jamming and spoofing, vessels should adopt precautionary measures, including the formulation of contingency communication plans and adherence to best practices concerning navigational systems. Specifically, it is advisable to incorporate GPS signal authentication mechanisms to counteract potential jamming and spoofing attacks. Additionally, enhancing the security of vessel communication systems can be achieved through the implementation of advanced encryption protocols. To proactively address cyber threats, vessels are encouraged to deploy intrusion detection systems that can identify and respond to potential security breaches (Kessler et al., 2018; Struck and Stoppe, 2021).

From an organizational standpoint, it is worth considering some useful insights drawn from this study. Examining the experiences of comparable industries, adopting and integrating a comprehensive cybersecurity framework tailored to maritime operations, such as the C2M2 and CSF frameworks (Gourisetti et al., 2020), which encompass identification, protection, detection, response, and recovery, appears advantageous. Given the prevalence of diverse cyber threats across various regions, sharing threat intelligence and implementing region-specific cybersecurity measures help enhance the overall resilience of the maritime industry (Meland et al., 2021). Collaborating with cybersecurity experts to develop and implement comprehensive cybersecurity policies and incident response plans is also advisable. Additionally, recognizing the geopolitical implications of cyber threats and advocating for international cooperation to strengthen global cybersecurity resilience is essential. Within this framework, fostering international collaboration, sharing information, and conducting joint exercises to address the transnational nature of cyber threats in the maritime domain can be effectively achieved. It is clear that there are still lessons to be gleaned from each incident. Given the limited history of maritime cyber threats and the tendency of some sectors to avoid reporting cyber-attacks to preserve their image and reputation, establishing clear and accessible channels for reporting cyber incidents is crucial to cultivate a culture of transparency and prompt response (Cormen, 2009). This necessitates bolstering international partnerships to exchange intelligence on threats and cooperate on strategies to mitigate cyber threats (Al Ali et al., 2021). In pursuit of this goal, backing cybersecurity education at the national level to improve the overall security stance of the maritime sector, and offering regular cybersecurity training for all personnel, along with ensuring employees are proficient in identifying signs of attacks, must all be enacted from an organizational standpoint (Ahvenjärvi et al., 2019).

Looking at the various technical and organizational measures outlined above, it is clear that successfully tackling cyber threats in the maritime sector necessitates a comprehensive approach covering both

Table 10
Research findings and outcomes comparison.

Literature	Gunes et al. (2021)	Uflaz et al. (2024)	Tam and Jones (2019)	Park et al. (2023b)	Svilicic et al. (2019)	Yoo and Park (2021)	Schauer et al. (2019)	Current paper
Cyber-attacks	B, D	A, B, C, D, G	A, B, C, G	A, B, D, E,	NP	NP	A, B, E, F	A-G
Type of data	Subjective	Subjective	Subjective	Subjective	Subjective	Subjective	Subjective	Objective
SRIF	4, 5, 6, 9, 10, 11	4, 5, 6, 9, 11	3, 4, 5, 6, 7, 9, 11	5, 9, 10, 11	4, 5, 6, 9, 10, 11	4, 6, 10, 11	3, 4, 5, 6, 7, 9, 10, 11	1–9
Target	SP	VS	VS	GN	VS	VS	GN	SP, SC, VS, OS, ED, SB, MO
Domain	Specific	General	General	General	Specific	General	General	Global
Importance ranking	No	Yes	No	Yes	Yes	Yes	Yes	Yes
Interdependency analysis	No	No	No	No	No	No	No	Yes
Implications	Technical	Technical	Technical	Technical, organizational	Technical	Technical, organizational	Technical, organizational	Technical, organizational

Cyber-attacks: (A: DDOS; B: Hacking; C: Jamming; D: Malware; E: Phishing; F: Ransomware; G: Spoofing; NP: No particular attack).
Target: (SP: Seaport; SC: Shipping company; VS: vessel; OS: Off-shore structures; ED: Energy distributers; SB: Shipbuilding firms; MO: Managerial organization; GN: General).
SRIF: (1. Region; 2. Country; 3. Perpetrator; 4. Scenario; 5. Cyber-attack type; 6. Target; 7. Successful attack; 8. Temporal trend; 9. Consequence; 10. Prevention ability; 11. Security risk level.
Domain: (Specific: Focusing on a case study; General: No particular case study; Global: applicable in a global scale).

technological and institutional angles. A multifaceted cybersecurity strategy that integrates robust technical safeguards along with organizational policies and procedures is vital for building a resilient defense system capable of withstanding the complex and rapidly advancing cyber threat landscape. No single solution can fully address the issue, but rather a combination of technical defenses and organizational processes working in tandem will be key to effectively counteracting cyberattacks targeting the maritime industry.

In summary, the current study pioneered the use of micro-level risk factors to quantify maritime cybersecurity risk levels, accurately reflecting real-world threats. By employing a data-driven analysis, it captured intricate dependencies and enabled quantitative analysis, enhancing statistical inference and model validation. The adaptable model, validated through various techniques, demonstrated efficacy and offered valuable insights, making it highly applicable in predicting and mitigating cybersecurity risks.

5.3. Future research directions

The potential future research directions of cybersecurity, with a focus on data-driven BN, involve several key areas. Firstly, there's an emphasis on advanced threat detection and prediction, utilizing sophisticated BN models integrated with real-time data sources and machine learning techniques. Additionally, data-driven BNs can enhance cyberattack attribution and forensic analysis, aiding in tracing the origin and methods of attackers more effectively. Integration with machine learning algorithms further strengthens predictive capabilities, while incorporating threat intelligence offers a context-aware approach to threat analysis and response. Finally, exploring BNs in human-centric security involves analyzing user behavior to identify insider threats. These research directions can contribute to the advancement of cybersecurity in the era of data-driven BN models, helping organizations better protect their digital assets and respond effectively to evolving cyber threats. Furthermore, there exists another prominent subject within the realm of maritime security that warrants consideration in future research endeavors. The concept of security is commonly categorized into two realms: physical security and cyber security. However, it is crucial to recognize that these domains are interconnected and should not be examined in isolation. A significant concern for the maritime industry is the coordinated use of both cyber and physical attacks to undermine its security. In such scenarios, the potential for causing substantial damage to the maritime supply chain and the resulting consequences is heightened. Looking back historically, the port of Antwerp experienced instances of combined cyber-physical attacks, where intruders infiltrated port offices, concealed advanced data interception devices such as key loggers, and subsequently exploited the breach to remotely access sensitive logistics data (Roberts, 2019). This incident underscores the importance of adopting a comprehensive perspective that considers potential vulnerabilities from various angles, rather than focusing solely on one aspect of security. In pursuit of this objective, future research should concentrate on pinpointing potential scenarios involving combined cyber-physical attacks, identifying vulnerabilities from diverse perspectives, creating a platform for a comprehensive assessment of risks associated with combined cyber-physical threats, formulating suitable security measures, and undertaking cost-benefit analyses.

6. Conclusion

This paper introduces an innovative approach to assessing cybersecurity risks in maritime infrastructures, including off-shore structures, seaports, shipping companies, and vessels. By conducting a thorough literature review and utilizing real data, based on the open-source MCAD database, which documents incidents of cyber threats in the maritime domain, the key SRIFs are identified, and a distinct data-driven BN model is constructed. The model assists in successfully analyzing the potential cybersecurity risks posed to different sectors of the maritime industry. The validation of the developed model involves employing a diverse set of techniques, including comparative, data splitting, metric and sensitivity analyses. The outcomes of these analyses affirm the model's strong robustness and reliability. In the examination of the cybersecurity model, ransomware emerges as the most prevalent form of cyber-attacks in stationary maritime infrastructures, followed by hacking, malware, phishing, and DDOS. For vessels, the predominant cyber threats consist of spoofing and jamming, in that order. Moreover, it becomes evident that three significant SRIFs—specifically, year, country, and target—exert substantial influence on the target node. Based on the results, it can be concluded that developed nations, while potentially spared from physical terrorist attacks, face cybersecurity threats that jeopardize their maritime infrastructures, especially shipping companies and seaports. The findings of the study provide valuable insights for stakeholders and government entities, contributing to a better comprehension of cybersecurity issues concerning various elements of the maritime industry. This knowledge has the potential to fortify preventive measures and improve emergency management strategies. Furthermore, the study highlights the necessity for additional exploration within maritime cybersecurity, outlining potential avenues for future research and indicating the limitations within existing studies. However, it is to be noted that the current study's limitation lies in its reliance on a relatively modest list of the recorded maritime cyber

incidents in the most comprehensive database in the field so far, which might not encompass all possible attack scenarios. To enhance the recognition and management of cyber threats in this sector, it is crucial to keep updating the database and consider integrating expert judgment, data-driven analysis, and insights from other relevant fields in future.

CRediT authorship contribution statement

Massoud Mohsendokht: Writing – review & editing, Writing – original draft, Validation, Software, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Huanhuan Li:** Writing – review & editing, Validation, Supervision, Software, Project administration, Methodology, Investigation, Conceptualization, Formal analysis, Visualization, Writing – original draft. **Christos Kontovas:** Writing – review & editing, Validation, Supervision, Investigation. **Chia-Hsun Chang:** Writing – review & editing, Validation, Supervision, Investigation. **Zhuohua Qu:** Writing – review & editing, Supervision, Investigation. **Zaili Yang:** Writing – review & editing, Validation, Supervision, Resources, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Zaili Yang reports financial support was provided by European Research Council. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work is supported by a European Research Council project (TRUST CoG 2019 864724).

References

Ahvenjärvi, S., et al., 2019. Safe information exchange on board of the ship. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 13 (1), 165–171. https://doi.org/10.12716/1001.13.01.17.

Al Ali, N.A.R., Chebotareva, A.A., Chebotarev, V.E., 2021. Cyber security in marine transport: opportunities and legal challenges. Pomorstvo 35 (2), 248–255. https://doi.org/10.31217/p.35.2.7.

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.

Amirkhani, H., Rahmati, M., Lucas, P.J.F., Hommersom, A., 2017. Exploiting experts' knowledge for structure learning of bayesian networks. IEEE Trans. Pattern Anal. Mach. Intell. 39 (11), 2154–2170. https://doi.org/10.1109/TPAMI.2016.2636828.

Ashraf, I., et al., 2022. A survey on cyber security threats in IoT-enabled maritime industry. IEEE Trans. Intell. Transport. Syst. 1–14. https://doi.org/10.1109/TITS.2022.3164678.

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. https://doi.org/10.3390/info13010022.

Benmalek, M., 2024. Ransomware on cyber-physical systems: taxonomies, case studies, security gaps, and open challenges. Internet Things Cyber-Phys. Syst 4, 186–202. https://doi.org/10.1016/j.iotcps.2023.12.001.

Berghout, T., Benbouzid, M., 2022. EL-NAHL: exploring labels autoencoding in augmented hidden layers of feedforward neural networks for cybersecurity in smart grids. Reliab. Eng. Syst. Saf. 226, 108680 https://doi.org/10.1016/j.ress.2022.108680.

BIMCO, 2018. The guidelines on cyber security onboard ships, version 4 [Online]. Available: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships.

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.

Bolbot, V., Kulkarni, K., Brunou, P., Banda, O.V., Musharraf, M., 2022. Developments and research directions in maritime cybersecurity: a systematic literature review and bibliometric analysis. Int. J. Crit. Infrastruct. Prot. 39, 100571 https://doi.org/10.1016/j.ijcip.2022.100571.

Boudehenn, C., Jacq, O., Lannuzel, M., Cexus, J.-C., Boudraa, A., 2021. Navigation anomaly detection: an added value for maritime cyber situational awareness. In: *2021 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, Dublin, Ireland. IEEE, pp. 1–4. https://doi.org/10.1109/CyberSA52016.2021.9478189.

Bouejla, A., Chaze, X., Guarnieri, F., Napoli, A., 2014. A Bayesian network to manage risks of maritime piracy against offshore oil fields. Saf. Sci. 68, 222–230. https://doi.org/10.1016/j.ssci.2014.04.010.

Caprolu, M., Pietro, R.D., Raponi, S., Sciancalepore, S., Tedeschi, P., 2020. Vessels cybersecurity: issues, challenges, and the road ahead. IEEE Commun. Mag. 58 (6), 90–96. https://doi.org/10.1109/MCOM.001.1900632.

Carreras Guzman, N.H., Wied, M., Kozine, I., Lundteigen, M.A., 2020. Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. Syst. Eng. 23 (2), 189–210. https://doi.org/10.1002/sys.21509.

Chang, C.-H., Kontovas, C., Yu, Q., Yang, Z., 2021. Risk assessment of the operations of maritime autonomous surface ships. Reliab. Eng. Syst. Saf. 207, 107324 https://doi.org/10.1016/j.ress.2020.107324.

Cheng, T., et al., 2024. Analysis of human errors in human-autonomy collaboration in autonomous ships operations through shore control experimental data. Reliab. Eng. Syst. Saf. 246, 110080 https://doi.org/10.1016/j.ress.2024.110080.

Cohen, J., 1960. A coefficient of agreement for nominal scales. Educ. Psychol. Meas. 20 (1), 37–46. https://doi.org/10.1177/001316446002000104.

Cormen, T.H., 2009. Introduction to Algorithms. MIT press.

Cover, T.M., Thomas, J.A., 2005. Elements of Information Theory, first ed. Wiley. https://doi.org/10.1002/047174882X.

De Neira, A.B., Kantarci, B., Nogueira, M., 2023. Distributed denial of service attack prediction: challenges, open issues and opportunities. Comput. Network. 222, 109553 https://doi.org/10.1016/j.comnet.2022.109553.

Diao, X., et al., 2024. Dynamic probabilistic risk assessment for electric grid cybersecurity. Reliab. Eng. Syst. Saf. 241, 109699 https://doi.org/10.1016/j.ress.2023.109699.

Fan, S., Yang, Z., 2024. Accident data-driven human fatigue analysis in maritime transport using machine learning. Reliab. Eng. Syst. Saf. 241, 109675 https://doi.org/10.1016/j.ress.2023.109675.

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.

Fan, S., Yang, Z., Wang, J., Marsland, J., 2022. Shipping accident analysis in restricted waters: lesson from the Suez Canal blockage in 2021. Ocean Eng. 266, 113119 https://doi.org/10.1016/j.oceaneng.2022.113119.

Freire, W.P., Melo, W.S., Do Nascimento, V.D., Nascimento, P.R.M., De Sá, A.O., 2022. Towards a secure and scalable maritime monitoring system using blockchain and low-cost IoT technology. Sensors 22 (13), 4895. https://doi.org/10.3390/s22134895.

Friedman, N., Geiger, D., Goldszmidt, M., 1997. Bayesian Network Classifiers. Machine Learning, 29, pp. 131–163. https://doi.org/10.1023/A:1007465528199.

Gourisetti, S.N.G., Mylrea, M., Patangia, H., 2020. Cybersecurity vulnerability mitigation framework through empirical paradigm: enhanced prioritized gap analysis. Future Generat. Comput. Syst. 105, 410–431. https://doi.org/10.1016/j.future.2019.12.018.

Gunes, B., Kayisoglu, G., Bolat, P., 2021. Cyber security risk assessment for seaports: a case study of a container port. Comput. Secur. 103, 102196 https://doi.org/10.1016/j.cose.2021.102196.

Hao, Z., Xu, Z., Zhao, H., Yang, L., 2023. Risk assessment model with probabilistic linguistic fuzzy inference methods for maritime piracy crime and applications. Appl. Soft Comput. 140, 110262 https://doi.org/10.1016/j.asoc.2023.110262.

Henriques De Gusmão, A.P., Mendonça Silva, M., Poleto, T., Camara E Silva, L., Cabral Seixas Costa, A.P., 2018. Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. Int. J. Inf. Manag. 43, 248–260. https://doi.org/10.1016/j.ijinfomgt.2018.08.008.

Hu, J.-L., Tang, X.-W., Qiu, J.-N., 2016. Assessment of seismic liquefaction potential based on Bayesian network constructed from domain knowledge and history data. Soil Dynam. Earthq. Eng. 89, 49–60. https://doi.org/10.1016/j.soildyn.2016.07.007.

IMO, 2022. Guidelines On Maritime Cyber Risk Management. MSC-FAL.1/Circ.3/Rev.2 [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2/20-/20Guidelines/20On/20Maritime/20Cyber/20Risk/20Management/20(Secretariat)/20(1).pdf.

Ji, Z., Xia, Q., Meng, G., 2015. A review of parameter learning methods in bayesian network. In: Huang, D.-S., Han, K. (Eds.), Advanced Intelligent Computing Theories and Applications, Vol. 9227, Lecture Notes in Computer Science, 9227. Springer International Publishing, Cham, pp. 3–12. https://doi.org/10.1007/978-3-319-22053-6_1.

Jiang, M., Lu, J., 2020. The analysis of maritime piracy occurred in Southeast Asia by using Bayesian network. Transport. Res. Part E Logist. Transp. Rev. 139, 101965 https://doi.org/10.1016/j.tre.2020.101965.

Jiang, L., Cai, Z., Wang, D., Zhang, H., 2012. Improving Tree augmented Naive Bayes for class probability estimation. Knowl.-Based Syst. 26, 239–245. https://doi.org/10.1016/j.knosys.2011.08.010.

Joseph, V.R., 2022. Optimal ratio for data splitting. Stat. Anal. Data Min. ASA Data Sci. J. 15 (4), 531–538. https://doi.org/10.1002/sam.11583.

Kabir, S., Papadopoulos, Y., 2019. Applications of Bayesian networks and Petri nets in safety, reliability, and risk assessments: a review. Saf. Sci. 115, 154–175. https://doi.org/10.1016/j.ssci.2019.02.009.

Kamal, B., Çakır, E., 2022. Data-driven Bayes approach on marine accidents occurring in Istanbul strait. Appl. Ocean Res. 123, 103180 https://doi.org/10.1016/j.apor.2022.103180.

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., Chang, C.-H., 2022. Maritime cybersecurity: are onboard systems ready? Marit. Pol. Manag. 1–19. https://doi.org/10.1080/03088839.2022.2124464.

Kavallieratos, G., Katsikas, S., Gkioulos, V., 2019. Cyber-attacks against the autonomous ship. In: Katsikas, S.K., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Antón, A., Gritzalis, S., Mylopoulos, J., Kalloniatis, C. (Eds.), *Computer Security*, Vol. 11387, Lecture Notes in Computer Science, 11387. Springer International Publishing, Cham, pp. 20–36. https://doi.org/10.1007/978-3-030-12786-2_2.

Kavallieratos, G., Spathoulas, G., Katsikas, S., 2021. Cyber risk propagation and optimal selection of cybersecurity controls for complex cyberphysical systems. Sensors 21 (5), 1691. https://doi.org/10.3390/s21051691.

Kessler, G.C., 2021. The CAN bus in the maritime environment – technical overview and cybersecurity vulnerabilities. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 15 (3), 531–540. https://doi.org/10.12716/1001.15.03.05.

Kessler, G.C., Craiger, P., Haass, J.C., 2018. A taxonomy framework for maritime cybersecurity: a demonstration using the automatic identification system. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 12 (3), 429–437. https://doi.org/10.12716/1001.12.03.01.

Komal, 2023. Fuzzy attack tree analysis of security threat assessment in an internet security system using algebraic t-norm and t-conorm. In: Engineering Reliability and Risk Assessment. Elsevier, pp. 53–64. https://doi.org/10.1016/B978-0-323-91943-2.00003-4.

Kong, D., Lin, Z., Li, W., He, W., 2024. Development of an improved Bayesian network method for maritime accident safety assessment based on multiscale scenario analysis theory. Reliab. Eng. Syst. Saf. 251, 110344 https://doi.org/10.1016/j.ress.2024.110344.

Landis, J.R., Koch, G.G., 1977. The measurement of observer agreement for categorical data. Biometrics 33 (1), 159. https://doi.org/10.2307/2529310.

Larsen, M.H., Lund, M.S., 2021. Cyber risk perception in the maritime domain: a systematic literature review. IEEE Access 9, 144895–144905. https://doi.org/10.1109/ACCESS.2021.3122433.

Laso, P.M., et al., 2022. ISOLA: an innovative approach to cyber threat detection in cruise shipping. In: Rocha, Á., Fajardo-Toro, C.H., Rodríguez, J.M.R. (Eds.), Developments and Advances in Defense and Security, Vol. 255, 255. Springer Singapore, Singapore, pp. 71–81. https://doi.org/10.1007/978-981-16-4884-7_7. Smart Innovation, Systems and Technologies.

Li, H., Ren, X., Yang, Z., 2023. Data-driven Bayesian network for risk analysis of global maritime accidents. Reliab. Eng. Syst. Saf. 230, 108938 https://doi.org/10.1016/j.ress.2022.108938.

Li, H., Yang, Z., 2023. Incorporation of AIS data-based machine learning into unsupervised route planning for maritime autonomous surface ships. Transp. Res. Part E Logist. Transp. Rev. 176, 103171 https://doi.org/10.1016/j.tre.2023.103171.

Li, H., Zhou, K., Zhang, C., Bashir, M., Yang, Z., 2024a. Dynamic evolution of maritime accidents: comparative analysis through data-driven Bayesian Networks. Ocean Eng. 303, 117736 https://doi.org/10.1016/j.oceaneng.2024.117736.

Li, H., Çelik, C., Bashir, M., Zou, L., Yang, Z., 2024b. Incorporation of a global perspective into data-driven analysis of maritime collision accident risk. Reliab. Eng. Syst. Saf. 249, 110187 https://doi.org/10.1016/j.ress.2024.110187.

Liang, X., Fan, S., Lucy, J., Yang, Z., 2022. Risk analysis of cargo theft from freight supply chains using a data-driven Bayesian network. Reliab. Eng. Syst. Saf. 226, 108702 https://doi.org/10.1016/j.ress.2022.108702.

Liu, K., Yu, Q., Yuan, Z., Yang, Z., Shu, Y., 2021. A systematic analysis for maritime accidents causation in Chinese coastal waters using machine learning approaches. Ocean Coast Manag. 213, 105859 https://doi.org/10.1016/j.ocecoaman.2021.105859.

Liu, K., Yu, Q., Yang, Z., Wan, C., Yang, Z., 2022. BN-based port state control inspection for Paris MoU: new risk factors and probability training using big data. Reliab. Eng. Syst. Saf. 224, 108530 https://doi.org/10.1016/j.ress.2022.108530.

MCAD, 2023. Maritime Cyber Attack Database. NHL Stenden University of Applied Sciences [Online]. Available: https://maritimecybersecurity.nl/.

Meland, P. Há, Bernsmed, K., Wille, E., Rødseth, Ø.J., Nesheim, D.A., 2021. A retrospective analysis of maritime cyber security incidents. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 15 (3), 519–530. https://doi.org/10.12716/1001.15.03.04.

Meng, H., An, X., Xing, J., 2022. A data-driven Bayesian network model integrating physical knowledge for prioritization of risk influencing factors. Process Saf. Environ. Protect. 160, 434–449. https://doi.org/10.1016/j.psep.2022.02.010.

Mohsendokht, M., Li, H., Kontovas, C., Chang, C., Qu, Z., Yang, Z., 2024. Enhancing maritime transportation security: a data-driven Bayesian network analysis of terrorist attack risks. Risk Anal. https://doi.org/10.1111/risa.15750 risa.15750.

Öğütçü, G., Testik, Ö.M., Chouseinoglou, O., 2016. Analysis of personal information security behavior and awareness. Comput. Secur. 56, 83–93. https://doi.org/10.1016/j.cose.2015.10.002.

Oruc, A., Gkioulos, V., Katsikas, S., 2022. Towards a cyber-physical range for the integrated navigation system (INS). J. Mar. Sci. Eng. 10 (1), 107. https://doi.org/10.3390/jmse10010107.

Park, C., Kontovas, C., Yang, Z., Chang, C.-H., 2023. A BN driven FMEA approach to assess maritime cybersecurity risks. Ocean Coast Manag. 235, 106480 https://doi.org/10.1016/j.ocecoaman.2023.106480.

Patriarca, R., Simone, F., Di Gravio, G., 2022. Modelling cyber resilience in a water treatment and distribution system. Reliab. Eng. Syst. Saf. 226, 108653 https://doi.org/10.1016/j.ress.2022.108653.

Powers, D.M.W., Powers, A., 2011. Evaluation: from precision, recall and F-measure to ROC, informedness, markedness & correlation. J. Mach. Learn. Technol. https://doi.org/10.9735/2229-3981.

Pristrom, S., Yang, Z., Wang, J., Yan, X., 2016. A novel flexible model for piracy and robbery assessment of merchant ship operations. Reliab. Eng. Syst. Saf. 155, 196–211. https://doi.org/10.1016/j.ress.2016.07.001.

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.

Ren, H., Guo, Q., 2023. Flexible learning tree augmented naïve classifier and its application. Knowl.-Based Syst. 260, 110140 https://doi.org/10.1016/j.knosys.2022.110140.

Roberts, F.S., 2019. From football to oil rigs: risk assessment for combined cyber and physical attacks. J. Benefit-Cost Anal. 10 (2), 251–273. https://doi.org/10.1017/bca.2019.15.

Schauer, S., Polemi, N., Mouratidis, H., 2019. MITIGATE: a dynamic supply chain cyber risk assessment methodology. J. Transp. Secur. 12 (1–2), 1–35. https://doi.org/10.1007/s12198-018-0195-z.

Schinas, O., Metzger, D., 2023. Cyber-seaworthiness: a critical review of the literature. Mar. Pol. 151, 105592 https://doi.org/10.1016/j.marpol.2023.105592.

Shannon, S., C.E. C. E., 1949. The Mathematical Theory of Communication. University of Illinois Press, Champaign, IL, USA.

Sheng, T., Weng, J., Shi, K., Han, B., 2024. Analysis of human errors in maritime accidents: a Bayesian spatial multinomial logistic model. J. Transport. Saf. Secur. 16 (6), 594–610. https://doi.org/10.1080/19439962.2023.2235323.

Struck, M.C., Stoppe, J., 2021. A backwards compatible approach to authenticate automatic identification system messages. In: 2021 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, Rhodes, Greece, pp. 524–529. https://doi.org/10.1109/CSR51186.2021.9527954.

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.

Tang, D., Fang, Y.-P., Zio, E., 2023. Vulnerability analysis of demand-response with renewable energy integration in smart grids to cyber attacks and online detection methods. Reliab. Eng. Syst. Saf. 235, 109212 https://doi.org/10.1016/j.ress.2023.109212.

Tunçel, A.L., Sezer, S.I., Elidolu, G., Uflaz, E., Akyuz, E., Arslan, O., 2024. A rule-based Bayesian network modelling under evidential reasoning theory for risk analysis of anchoring operation in maritime transportation. Ocean Eng. 292, 116521 https://doi.org/10.1016/j.oceaneng.2023.116521.

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 (2), 208–227. https://doi.org/10.1057/s41278-022-00214-0.

Uflaz, E., Sezer, S.I., Tunçel, A.L., Aydin, M., Akyuz, E., Arslan, O., 2024. Quantifying potential cyber-attack risks in maritime transportation under Dempster–Shafer theory FMECA and rule-based Bayesian network modelling. Reliab. Eng. Syst. Saf. 243, 109825 https://doi.org/10.1016/j.ress.2023.109825.

UNCTAD, 2022. Review of Maritime Transport. United Nations Conference on Trade and Development (UNCTAD) [Online]. Available: https://unctad.org/rmt2022.

Wang, L., Yang, Z., 2018. Bayesian network modelling and analysis of accident severity in waterborne transportation: a case study in China. Reliab. Eng. Syst. Saf. 180, 277–289. https://doi.org/10.1016/j.ress.2018.07.021.

Weng, J., Du, J., Shi, K., Liao, S., 2023. Effects of ship domain shapes on ship collision risk estimates considering collision frequency and severity. Ocean Eng. 283, 115070 https://doi.org/10.1016/j.oceaneng.2023.115070.

Wu, J., 2018. A generalized tree augmented naive Bayes link prediction model. J. Comput. Sci. 27, 206–217. https://doi.org/10.1016/j.jocs.2018.04.006.

Xu, X., Wu, B., Man, J., Soares, C.G., 2024. Bayesian network modelling for navigation status control of cargo ships in the Three Gorges Waterway. Reliab. Eng. Syst. Saf. 245, 110018 https://doi.org/10.1016/j.ress.2024.110018.

Yang, Z., Yang, Z., Yin, J., 2018. Realising advanced risk-based port state control inspection using data-driven Bayesian networks. Transport. Res. Part Policy Pract 110, 38–56. https://doi.org/10.1016/j.tra.2018.01.033.

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., Yang, Z., Wang, H., Yang, Z., 2021. Geometrical risk evaluation of the collisions between ships and offshore installations using rule-based Bayesian reasoning. Reliab. Eng. Syst. Saf. 210, 107474 https://doi.org/10.1016/j.ress.2021.107474.

Zhang, D., Yan, X.P., Yang, Z.L., Wall, A., Wang, J., 2013. Incorporation of formal safety assessment and Bayesian network in navigational risk estimation of the Yangtze River. Reliab. Eng. Syst. Saf. 118, 93–105. https://doi.org/10.1016/j.ress.2013.04.006.

Zhou, K., Xing, W., Wang, J., Li, H., Yang, Z., 2024. A data-driven risk model for maritime casualty analysis: a global perspective. Reliab. Eng. Syst. Saf. 244, 109925 https://doi.org/10.1016/j.ress.2023.109925.

Netica (version 607). Norsys Software Corp, 2019 [Online]. Available: https://www.norsys.com/index.html.