Reliability Engineering and System Safety 279 (2027) 113823



Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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



MC-QRA: quantitative spatiotemporal risk assessment and probabilistic dependency analysis of maritime cyber attacks

Jincheng Gong [a], Yunfeng Zhao [b], Huanhuan Li [c,*], Zaili Yang [b,*]

[a] School of Mechanical and Electrical Engineering, University of Electronic Science and Technology of China, Chengdu, China
[b] Liverpool Logistics, Offshore and Marine (LOOM) Research Institute, Liverpool John Moores University, Liverpool, UK
[c] School of Engineering, University of Southampton, Southampton, UK

ARTICLE INFO

Keywords:
Maritime cybersecurity
Quantitative risk assessment
Latent class analysis
Spatiotemporal analysis
Probabilistic dependency analysis

ABSTRACT

The increasing digitalisation of maritime systems has raised concerns about cyber threats to shipping operations, port infrastructure and maritime safety. However, existing approaches often examine cyber-risk scenarios, geographical patterns and dependencies among risk factors separately. This study proposes Maritime Cyber-Quantitative Risk Assessment (MC-QRA), an integrated framework for scenario-based relative risk assessment, spatiotemporal analysis and probabilistic dependency modelling using reported maritime cyber incidents. The framework comprises four stages: latent class analysis (LCA) for scenario identification; frequency–severity scoring for relative risk assessment; kernel density estimation (KDE) and Getis–Ord Gi* analysis for spatiotemporal assessment; and mutual information (MI) and Tree-Augmented Naive Bayes (TAN) modelling for dependency analysis. The framework was applied to 444 incidents from the Maritime Cyber Attack Database (MCAD), identifying five distinct cyberattack scenarios. The results show an increase in reported incidents classified as medium or high risk after 2021, with risk-weighted spatial concentrations in Europe, North America and East Asia. Scenario-level risk decomposition indicates that ransomware-related incidents account for 52.2% of the summed relative risk scores, compared with 19.6% for spoofing-related incidents. Cyber threat type, exploited asset and target category provide the most information for distinguishing the assigned risk levels. The TAN model achieved a mean classification accuracy of 87.4% under stratified fivefold cross-validation, while identifying conditional probabilistic dependencies among incident characteristics. The resulting risk indices and spatial patterns describe relative differences within the reported MCAD sample rather than exposure-adjusted absolute risk. MC-QRA thus provides an integrated basis for comparing incident scenarios, examining spatiotemporal patterns and supporting preliminary maritime cyber-risk prioritisation.

1. Introduction

The maritime industry has undergone substantial digitalisation alongside the growth of global maritime trade [1]. Information and communication technologies are increasingly integrated into maritime transport operations [2], port logistics [3], and intelligent vessels [4], improving operational efficiency, connectivity and situational awareness. However, the growing interconnection of digital and physical systems also expands potential cyberattack surfaces across vessels, ports and supporting infrastructure, introducing vulnerabilities that may affect operational continuity, maritime safety and supply-chain reliability [5–7].

Maritime cybersecurity incidents represent low-frequency but potentially high-consequence events that can propagate across interconnected technical, organisational, and geographical boundaries [8]. Cyber incidents may lead not only to direct navigational hazards but also to cascading operational failures, including port shutdowns, cargo handling disruption, schedule delays, and broader impacts on global supply chains. Such characteristics position maritime cybersecurity as a critical concern.

Recent incidents underscore the severity of these risks. The suspected cyber-induced collision of two oil tankers in the Gulf of Oman on June 17, 2025, attributed to interference with Global Positioning System (GPS) and Automatic Identification System (AIS) signals, illustrates how cyber threats can directly compromise navigational safety in geopolitically sensitive regions [9]. Similarly, the 2025 cyberattack on the Port of

* Corresponding authors.
E-mail addresses: Huanhuan.Li@soton.ac.uk (H. Li), Z.Yang@ljmu.ac.uk (Z. Yang).

https://doi.org/10.1016/j.ress.2026.113823
Received 17 June 2026; Received in revised form 2 November 2026; Accepted 5 November 2026
Available online 6 November 2026
0951-8320/© 2026 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

Trieste, Italy, disrupted port operations and exposed the vulnerability and strategic significance of critical port infrastructure amid geopolitical tensions [10]. These events demonstrate that maritime cyber risk is not merely an information security issue, but a systemic safety and resilience challenge requiring multi-dimensional, dependency-aware assessment to facilitate the implementation of proper cybersecurity measures in a cost-effective manner.

Current research on maritime cybersecurity has provided valuable descriptive insights, but it often considers a limited set of dimensions. Existing studies predominantly rely on literature reviews, case analyses, and questionnaire-based approaches, while data-driven methods with multi-dimensional analysis remain relatively scarce, as highlighted in the systematic review in Section 2. For example, Akpan et al. [11] systematically reviewed maritime cybersecurity incidents, identifying vulnerable ship systems and summarising representative attack cases, while Afenyo and Caesar [12] similarly highlighted persistent research gaps in data monitoring, economic impact assessment, and regulatory frameworks. Survey-based studies using structural equation modelling have further examined organisational and human factors, identifying training and awareness as influential determinants of cybersecurity performance. However, these approaches primarily capture perceptions, high-level trends, or isolated cases, and offer limited support for multi-dimensional risk comparison, spatiotemporal pattern identification, or Risk Influential Factors (RIFs) interdependency-aware inference [13].

As a result, several critical challenges remain unresolved: (i) the lack of multi-dimensional frameworks for maritime cybersecurity risk assessment, capable of jointly modelling cyberattack likelihood and consequence severity; (ii) insufficient understanding of the spatiotemporal evolution of reported maritime cyber incidents; and (iii) limited capability to identify and interpret probabilistic dependencies among risk factors within complex maritime systems. These gaps constrain the ability of researchers and practitioners to move from descriptive assessments towards predictive, preventive, and decision-oriented cyber risk management.

To address these challenges, this study develops Maritime Cyber-Quantitative Risk Assessment (MC-QRA), a data-driven framework for examining cyber-risk patterns in reported maritime incidents. Using records from the Maritime Cyber Attack Database (MCAD) [14], the framework combines scenario identification, frequency–severity risk assessment, spatiotemporal analysis and probabilistic dependency modelling. It is designed to compare relative risk across heterogeneous attack scenarios, examine changes in the geographical and temporal distribution of reported incidents, and identify statistical relationships among RIFs.

MC-QRA builds on established methods rather than introducing new algorithms. Latent class analysis (LCA) is used to identify representative attack scenarios, which are compared using a frequency–severity risk index. Kernel density estimation (KDE) and Getis–Ord Gi* analysis are applied to examine geographical concentrations and their temporal variation. Mutual information (MI) and Tree-Augmented Naive Bayes (TAN) modelling are used to assess the information provided by individual RIFs and the conditional probabilistic dependencies among them. The resulting risk measures are relative to the MCAD sample and do not represent exposure-adjusted probabilities or absolute risk.

The framework draws on the MCAD dataset and the RIF taxonomy developed by Zhao et al. [15], and the TAN-based dependency-analysis idea is related to Mohsendokht et al. [8]. Its methodological contribution is to generate a consistent assessment procedure that links scenario characteristics, relative risk scores, spatiotemporal patterns and probabilistic dependencies.

The major contributions of this study are as follows:

(1) A unified MC-QRA framework is proposed that integrates quantitative risk measurement, spatiotemporal risk analysis, and dependency modelling within a three-dimensional analytical structure. The framework provides a systematic basis for understanding the magnitude and evolution of maritime cyber risk and the probabilistic dependencies among risk-related factors, supporting risk-informed decision-making for maritime cyber-physical systems.
(2) A scenario-based quantitative risk assessment methodology is developed for maritime cyber incidents by integrating LCA-based clustering with a frequency–severity risk formulation. This approach enables the systematic representation of heterogeneous cyberattack scenarios and provides comparable within-sample relative risk indices and ordinal risk levels across different reported attack types in the MCAD.
(3) A spatiotemporal risk mining approach is proposed by combining KDE and Getis–Ord Gi* hotspot analysis to identify spatial concentrations, temporal trends, and emerging high-risk regions of maritime cyber incidents, thereby extending cyber-risk assessment beyond static or case-specific analyses.
(4) A dependency-aware risk modelling approach is established using a TAN model to capture probabilistic relationships among RIFs and to infer conditions associated with elevated maritime cyber risk.

The remainder of this paper is organised as follows. Section 2 reviews prior studies on maritime cybersecurity and risk assessment, summarising theoretical foundations, methodological progress, and current limitations in data, modelling, and interpretation. Section 3 presents the overall design of the MC-QRA framework, detailing processes for data handling, scenario classification, risk quantification, and spatiotemporal analysis. Section 4 reports empirical results derived from the MCAD data. Section 5 discusses theoretical and practical implications and future directions, and Section 6 concludes with a summary and highlights the key findings.

2. Literature review

This study uses CiteSpace to examine the development of maritime cyberattack risk research and identify gaps in the existing literature. The keyword clustering and timeline analyses are presented in Appendix A, and their findings are discussed in Sections 2.1–2.3 to inform the development of the proposed MC-QRA framework. Conventional risk assessment methods are also critically reviewed and compared to identify their limitations in addressing the multidimensional and spatiotemporal characteristics of maritime cyber risks, particularly the dependencies among RIFs. These findings establish the methodological basis for the proposed framework and clarify how it addresses limitations in existing maritime cybersecurity risk assessment approaches.

2.1. Research progress of cybersecurity

A systematic search was conducted via the Web of Science (WoS) database [16] using the keyword “Maritime Cybersecurity” in August 2025, yielding a total of 301 publications indexed in core journals. CiteSpace [17] was subsequently utilised to construct a keyword co-occurrence network and a temporal evolution map. These maps are used to trace dominant research themes and to reveal dimensions that remain insufficiently addressed in current maritime cybersecurity research.

Among the 301 retrieved publications, only three were published before 2015. Accordingly, the keyword clustering results in Fig. A-1 in the Appendix are illustrated for the period 2015–2025. The identified clusters can be broadly grouped into two dimensions: methodological approaches and research themes.

From a methodological perspective, key analytical approaches in maritime cybersecurity include Deep Learning (DL) (Cluster #0), Machine Learning (ML) (Cluster #1), and BNs (Cluster #4). These approaches represent the primary quantitative tools used in current

maritime cybersecurity research. However, the CiteSpace trend analysis also indicates that these methods are largely developed for detection, classification, or isolated subsystem risk assessment, while integrated multi-dimensional risk assessment remains less developed.

DL (Cluster #0) has been widely employed in maritime cybersecurity owing to its superior capability for feature extraction and pattern recognition, particularly in network intrusion detection. For example, Ali et al. [18] proposed a detection approach based on a deep encoder-decoder Artificial Neural Network (ANN) to identify intrusions and mitigate their effects, thereby maintaining system control and operational stability. Similarly, Kumar et al. [19] developed an automated framework for Cyber Threat Intelligence (CTI) modelling and threat-type identification, integrating deep feature extraction, CTI-driven detection, and CTI-based classification to achieve efficient and accurate defence performance. Although DL improves detection performance, it rarely links detected events to consequence severity, spatiotemporal risk concentration, or dependency structures among risk factors.

ML (Cluster #1) also plays a critical role in maritime cyber threat detection. Popli et al. [20] proposed a federated learning framework for underwater drone networks, enabling collaborative intrusion detection while preserving data privacy. The framework effectively addresses the challenges of low bandwidth and high security risks in the Internet of Underwater Things (IoUT). Wilson et al. [21] introduced a multi-agent reinforcement learning framework for autonomous cyber defence in industrial control systems. Diaz et al. [22] examined the applications of artificial intelligence and ML in maritime supply chain security under digital transformation, emphasising the potential roles of unmanned aerial systems and cryptography in enhancing cybersecurity and shipbuilding resilience. BN studies provide probabilistic dependency modelling, but most remain confined to specific subsystems or simplified scenarios, with limited use of large-scale incident data and spatiotemporal attributes.

The BN (Cluster #4) approach has been extensively applied in maritime cyber risk assessment for uncertainty modelling and probabilistic reasoning. Aydin et al. [23] conducted a probabilistic risk assessment of cyber threats targeting Maritime Autonomous Surface Ships (MASS) using an improved Z-number theory combined with BN. Their study revealed substantial cyberattack risks during open-sea navigation and offered valuable insights for risk mitigation. Uflaz et al. [24] proposed a probabilistic framework integrating BNs and Dempster-Shafer theory to evaluate cyber risks in ship bridge navigation systems, identifying AIS spoofing and GPS interference as critical threats and providing a foundation for enhanced maritime cybersecurity management.

With the continuous advancement of cybersecurity technologies, DL, ML, and BNs have become the core methodological paradigms in maritime cybersecurity. The progress of these techniques has helped address key challenges in cybersecurity (Cluster #3) and risk assessment (Cluster #2), thereby improving maritime safety and security protection.

Cybersecurity (Cluster #3) focuses on safeguarding maritime information systems against diverse threats and attacks, particularly within digitalised and intelligent transport systems. Haugli-Sandvik et al. [25] conducted a quantitative study on deck officers' perceptions of Information Technology (IT) and Operational Technology (OT) system risks, revealing that perceived benefits, cybersecurity training, and prior attack experience significantly influence risk perception. Soner and Kandemir [26] analysed the implementation and regulation of IT and OT technologies using the Analytic Hierarchy Process (AHP) to identify future maritime cybersecurity skill requirements. Their findings bridge the gap between current workforce competencies and the evolving needs of maritime transport systems, thereby strengthening overall safety and security standards.

Risk Assessment (Cluster #2) represents a key process for systematically identifying and evaluating potential threats, analysing their impacts, and designing mitigation strategies. In Cyber-Physical Systems (CPSs), Svilicic et al. [27] developed and verified a ship cybersecurity risk assessment process combining computational vulnerability scanning with quantitative risk analysis, effectively evaluating the cybersecurity of critical onboard systems. Despite these advances, most maritime-focused studies stop short of integrating spatiotemporal dynamics and probabilistic dependency into Quantitative Risk Assessment (QRA) frameworks.

As illustrated in Fig. A-2 in the Appendix, the evolution of maritime cybersecurity research has proceeded through distinct stages. Between 2015 and 2020, studies within the cybersecurity domain (Cluster #3) expanded significantly, focusing primarily on risk perception and skills training. From 2020 to 2025, research emphasis shifted towards methodological innovation, particularly the application of ML (Cluster #1) in intrusion detection, which emerged as a dominant trend. For example, Li et al. [28] proposed an edge federated learning-based intrusion detection framework integrating Convolutional Neural Networks (CNN) and Gated Recurrent Unit (GRU) models to achieve efficient, privacy-preserving threat identification in maritime Internet of Things (IoT) environments. Similarly, Liu et al. [29] introduced a CNN-Multi-Layer Perceptron (MLP) intrusion detection model (Fed-Batch) trained through federated learning. This approach enhances detection efficiency while maintaining data privacy and incorporates an adaptive batch aggregation mechanism to optimise the federated learning process in maritime IoT systems.

Although these approaches have improved detection efficiency, the CiteSpace analysis highlights three areas that remain insufficiently explored: (i) scenario-based quantitative risk assessment informed by empirical incident data, (ii) the spatial distribution and temporal evolution of cyber risks, and (iii) probabilistic dependencies among RIFs. These gaps, discussed further in Section 2.3, underpin the three analytical components of the proposed MC-QRA framework: LCA for scenario classification and frequency–severity-based risk quantification, KDE and Getis–Ord Gi* statistics for spatiotemporal hotspot analysis, and Mutual Information (MI) and TAN modelling to characterise dependencies among RIFs.

2.2. *Quantitative assessment methods for cybersecurity*

Cybersecurity risk assessment aims to identify, analyse, and quantify potential threats to information systems and CPSs to support effective protection strategies and risk-informed decision-making. Representative quantitative assessment approaches include Bayesian Networks (BNs), Bow-Tie analysis, Failure Modes and Effects Analysis/Failure Modes, Effects, and Criticality Analysis (FMEA/FMECA), Fault Tree Analysis (FTA), and QRA, as summarised in Table 1.

BN-based approaches provide a probabilistic means of representing uncertainty and dependencies in complex systems [50]. They have been applied in areas such as the Internet of Vehicles, autonomous vehicles, smart grids, water treatment systems, and other CPS applications. Previous studies show that BNs are useful for modelling conditional relationships between system components, updating probabilities when new evidence becomes available, and supporting predictive risk analysis. In cybersecurity studies, BNs have been used to assess attack impacts, support defensive resource allocation, and estimate the physical consequences of cyber incidents in CPSs, particularly in energy and power systems [24,30–37]. Although these studies demonstrate the value of BNs for dependency-aware modelling, many are limited to specific subsystems or simplified scenarios.

Bow-Tie analysis combines fault trees and event trees to describe threats, preventive barriers, escalation paths, and mitigation measures within a single framework. The method has been applied in maritime and industrial settings to examine cyber–physical attack pathways and relate attack likelihood to consequence severity [38–40]. A major advantage of Bow-Tie analysis lies in its clear visual structure and ease of interpretation. However, the method is generally static and depends

Table 1
Quantitative assessment methods for cybersecurity.

Method	Refs.	Advantages	Limitations
BN	Bitit et al. [30], Mahendran et al. [31], Tanwar et al. [32], Zhang and Zhang [33], Deng et al. [34], Le et al. [35], Gaskova and Massel [36], Park et al. [37], Uflaz et al. [24],	BN effectively models dependencies and quantifies uncertainties among cyber risk factors, enabling probabilistic reasoning and dynamic risk prediction in complex security systems.	Model construction depends heavily on expert knowledge and reliable data, and the computational cost increases sharply with network scale and complexity.
Bow-Tie	Papageorgiou et al. [38], Progoulakis et al. [39], Bemsmed et al. [40]	Bow-Tie provides an intuitive visualisation of threats, preventive barriers, and mitigation measures, helping to identify weak points and communicate cybersecurity risks clearly.	It is mainly qualitative and static, with limited capability to capture multi-stage or time-dependent cyberattack processes.
FTA	Fovino et al. [41], Nascimento et al. [42], Niloofar and Lazarova-Molnar [43], Kumar and Stoelinga [44], Weglian et al. [45]	FTA systematically traces root causes of cyber incidents through logical reasoning, supporting structured vulnerability identification and reliability validation.	It assumes fixed logical relationships and struggles to represent dynamic, interdependent, or probabilistic cyber threats.
QRA	Zhang et al. [46], Son et al. [47], Zhou et al. [48], Alguliyev et al. [49]	QRA quantitatively evaluates the probability and consequence of cybersecurity events, supporting data-driven prioritisation of security controls and investment decisions.	Its accuracy relies on high-quality data, and simplified assumptions may not fully capture complex attacker behaviours or system interactions.
FMEA/ FMECA	Park et al. [37], Uflaz et al. [24]	FMEA/FMECA identifies potential failure or compromise modes and emphasises preventive measures, suitable for proactive cybersecurity risk management.	It involves subjective judgments and lacks the ability to model interdependencies or handle uncertainty without integration with probabilistic methods.

heavily on expert judgement when defining causal relationships and barriers.

FTA is a top-down analytical method used to identify the root causes of system failures. In cybersecurity research, FTA has been extended through integration with attack trees and stochastic modelling approaches [41–45]. In CPS studies, it has been used to analyse attack propagation, coupled failures, and human–machine interaction problems. While FTA is effective for structural analysis, most applications assume fixed logical relationships and offer limited capability for representing dynamic changes in threat conditions.

QRA applies statistical and mathematical techniques to estimate both the likelihood and consequences of hazardous events and has been widely adopted for the assessment of critical digital assets and CPS infrastructures [46,47]. Some studies incorporate semi-quantitative scoring methods and protection-layer concepts to estimate attack probabilities and evaluate safeguards. Fuzzy-theory-based extensions have also been introduced to address uncertainty and imprecision in complex environments [48,49]. Nevertheless, many QRA studies rely on predefined parameters and do not explicitly account for dependencies among risk factors.

FMEA and FMECA are systematic methods for identifying potential failure modes and evaluating their effects and criticalities [51]. These methods are increasingly combined with probabilistic techniques to improve uncertainty handling. In maritime cybersecurity research, hybrid FMEA/FMECA-BN approaches have been used to assess navigation-system vulnerabilities and prioritise critical cyber threats [24,37]. Although such approaches improve failure prioritisation, they remain largely focused on individual components rather than broader system interactions.

The existing quantitative methods offer different strengths in probabilistic reasoning, structural analysis, and consequence assessment. Recent studies increasingly adopt hybrid approaches that combine multiple techniques. However, most existing work focuses either on general CPS applications or on isolated maritime subsystems. In addition, many studies remain constrained by limited use of large-scale incident data, static modelling assumptions, and insufficient consideration of spatiotemporal evolution and interdependent risk relationships.

Therefore, there remains a need for a unified and data-driven framework for maritime cybersecurity assessment that can support scenario-level risk characterisation, spatiotemporal risk evolution, and dependency-aware analysis of influential risk factors. This gap forms the basis for the MC-QRA framework proposed in this study.

2.3. Research gaps

The bibliometric analysis presented in Section 2.1 and the Appendix, together with the methodological review in Section 2.2, highlights three gaps in the assessment of maritime cyber risk.

(1) Limited scenario-based risk quantification using empirical incident data.

Much of the existing literature focuses on qualitative assessments, expert judgement or individual case studies [52]. Although incident databases provide opportunities for empirical analysis, comparatively little attention has been given to identifying heterogeneous attack scenarios and systematically comparing their associated risks. In particular, approaches that combine scenario frequency and consequence severity to derive consistent, data-driven risk measures remain limited. This restricts the comparative assessment and prioritisation of different types of reported maritime cyber incidents.

(2) Limited analysis of probabilistic dependencies among RIF.

Existing studies have examined individual risk factors and their associations with maritime cyber incidents, but the conditional dependencies among incident characteristics and assigned risk levels remain insufficiently explored. Analyses based primarily on marginal frequencies or pairwise associations may overlook relationships that emerge when several factors are considered jointly. Probabilistic

dependency modelling could therefore provide additional insight into how combinations of RIFs are associated with different risk levels, without implying causal relationships.

(3) Insufficient integration of spatial and temporal patterns into cyber-risk assessment.

Maritime cyber-risk studies have generally placed greater emphasis on specific incidents, systems or operational contexts than on the geographical distribution and temporal variation of reported cyber risk. Consequently, spatial concentrations, statistically significant clusters and changes in their distribution over time have received comparatively limited attention. Integrating spatial and temporal analyses with incident-level risk measures would provide a more detailed account of where and when higher-scoring incidents are concentrated, while recognising the influence of reporting coverage and differences in maritime cyber exposure.

3. Methodology

This section describes the methodological structure and analytical workflow of the MC-QRA framework. The framework is designed to support empirical, spatiotemporal, and dependency analysis of maritime cybersecurity risk using incident-level data. MC-QRA consists of four sequential components: scenario classification, risk assessment, spatiotemporal risk analysis, and BN-based analysis.

3.1. Overall framework

In this study, multi-dimensional risk analysis refers to the joint consideration of (i) risk composition (frequency and severity), (ii) spatiotemporal variation, and (iii) interdependencies among RIFs. The analysis is based on the MCAD developed by Zhao et al. [15]. The MC-QRA workflow is outlined in four consecutive stages in Fig. 1, each addressing a specific analytical objective within the risk assessment process.

(1) Scenario identification. LCA clustering is applied to the processed dataset to group cyber incidents into representative attack scenarios based on discrete RIFs. This step produces a finite set of scenario categories and their corresponding occurrence frequencies, enabling aggregation and comparison of cyber risks across different attack patterns.

(2) Risk assessment. Scenario-level risk is quantified by combining occurrence frequency with consequence severity indicators derived from the associated RIFs. This formulation yields comparable risk scores across scenarios and provides a basis for ranking cyberattack types according to their relative threat levels.

(3) Spatiotemporal risk analysis: Using the computed risk scores, KDE and Getis–Ord Gi* statistics are employed to examine the spatial distribution of cyber risks. Temporal information is incorporated to analyse changes in spatial concentration and risk intensity over time, allowing identification of persistent and emerging high-risk regions.

(4) Probabilistic dependency analysis: To investigate relationships between RIFs and maritime cyber risk levels, MI is first employed to identify the most informative variables. A TAN model is then developed to capture conditional dependencies among RIFs and risk outcomes. Spatiotemporal attributes are incorporated into the BN as additional RIFs, allowing the influence of temporal dynamics and spatial heterogeneity on maritime cyber risk to be explicitly represented. The resulting model facilitates probabilistic inference and dependency analysis, enabling the identification and interpretation of factor interactions associated with high-risk and very-high-risk scenarios.

Overall, the MC-QRA framework provides a structured methodology

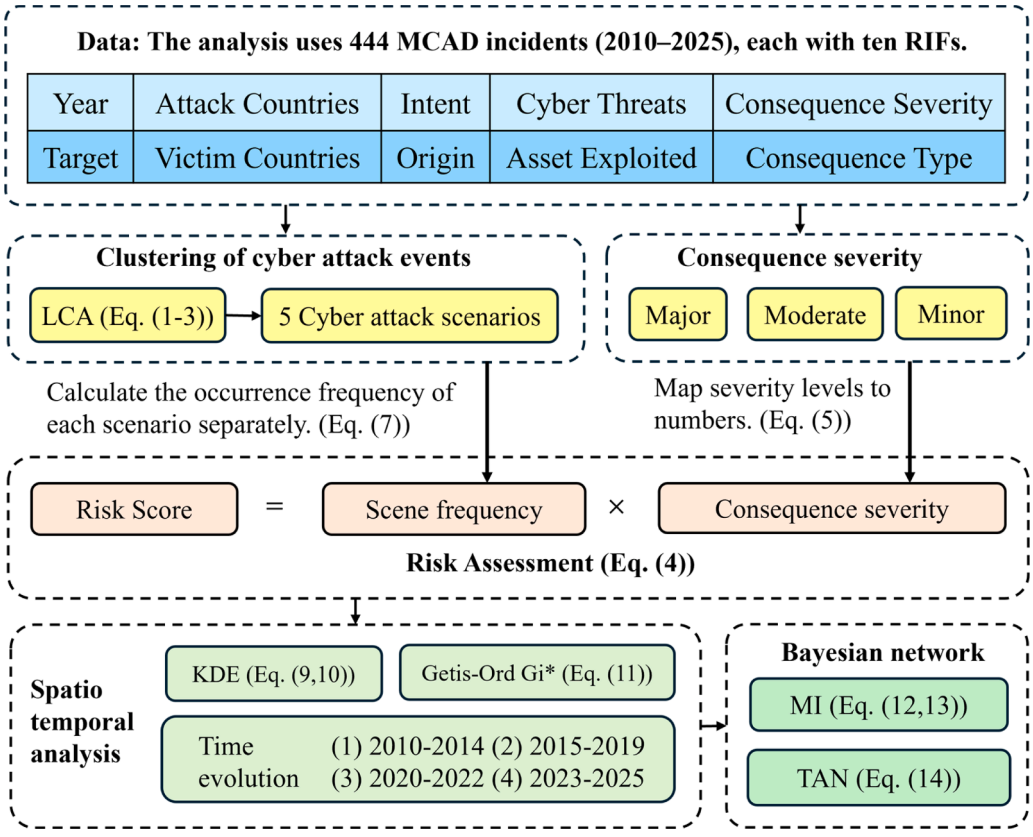


Fig. 1. The overall framework of MC-QRA.

for transforming heterogeneous cyber incident records into multi-dimensional, spatiotemporal, and risk-factor dependency-aware representations, suitable for subsequent analysis and decision support.

3.2. Risk factor identification and scenario clustering

Following the variable classification scheme proposed by Zhao et al. [15], ten RIFs were selected for each maritime cyber incident: Year, Attack Countries, Victim Countries, Target, Cyber Threats, Consequence Severity, Intent, Origin, Asset Exploited, and Consequence Type. These factors were selected to provide a structured description of each incident rather than a minimal set of statistically independent predictors. They capture the temporal context, attack characteristics, exposure conditions, and consequences of maritime cyber incidents.

Let the processed dataset be denoted as $X_{RIF} = \{x^1, x^2, \ldots x^m\}$, where each incident $x^i = \{x_1^i, x_2^i, \ldots, x_n^i\}$ is described by n discrete RIFs. To identify representative cyberattack scenarios at a macro level, the LCA clustering algorithm [53] was applied to classify the dataset into K latent classes $\{C_1, C_2, \ldots, C_K\}$. LCA was chosen because it accommodates categorical variables and provides a probabilistic description of class membership. Rather than relying solely on a distance measure, it estimates the probability of each observed RIF category within a latent class and assigns incidents according to their posterior class probabilities. This also allows uncertainty in scenario classification to be examined. Each class is characterised by a distinct profile of conditional probabilities across the ten RIFs.

LCA assumes that the observed RIFs are conditionally independent given the latent class. Let $z_i \in \{1, \ldots, K\}$ denote the latent class of incident i. The marginal probability of an incident is:

$$P(x^i) = \sum_{k=1}^{K} \pi_k \prod_{j=1}^{n} P\left(x_j^i \middle| z_i = k\right) \tag{1}$$

where $\pi_k = P(z_i = k)$ is the class prevalence, and $P\left(x_j^i \middle| z_i = k\right)$ is the conditional probability of the j-th RIF in class k.

The model parameters are estimated using the Expectation–Maximisation (EM) algorithm. In the E-step, the posterior probability of incident (i) belonging to class (k) is calculated as:

$$P(z_i = k|x^i) = \frac{\pi_k \prod_{j=1}^{n} P\left(x_j^i \middle| z_i = k\right)}{\sum_{l=1}^{K} \pi_l \prod_{j=1}^{n} P\left(x_j^i \middle| z_i = l\right)} \tag{2}$$

In the M-step, the class prevalences and conditional category probabilities are re-estimated using these posterior probabilities as weights. The two steps are repeated until convergence of the log-likelihood. Each incident is subsequently assigned to the class with the highest posterior probability:

$$z^i = \arg\max_{k=1,\ldots,K} P(z_i = k|x^i) \tag{3}$$

The number of latent classes K was determined by comparing LCA with alternative categorical clustering methods and by evaluating model fit, class separation, and interpretability. The pseudocode for LCA is shown in Algorithm 1.

Algorithm 1: LCA algorithm

Input: Dataset X_{RIF}, Number of latent classes K, Maximum iterations T
Output: Cluster prevalences π_k, Conditional probabilities $P(x_j|z = k)$, Cluster assignments z^i.
Initialise π_k and $P(x_j|z = k)$, using multiple random starts.
for iteration $t = 1, 2, \ldots, T$:
E-step: for each $x^i \in X_{RIF}$, compute $P(z_i = k|x^i)$ for $k = 1, \ldots, K$
M-step: update $\pi_k = (1/m)\sum_i P(z_i = k|x^i)$
for each RIF_j, update $P(x_j|z = k)$ as the posterior-weighted
Empirical distribution of x_j in class k

(continued on next column)

(continued)

Algorithm 1: LCA algorithm

Compute log-likelihood $L = \sum_{i=1}^{m} \log P(x^i)$
if L change between consecutive iterations $<$ convergence criterion:
break
Assign $z^i = \max_k P(z_i = k|x^i)$

3.3. Quantitative macro-level risk assessment

In safety engineering, risk is conventionally characterised as a function of event likelihood (F) and consequence severity (CS), providing a quantitative basis for comparing heterogeneous hazards. Following this principle, the maritime cybersecurity risk score for an incident is S_{risk}^i defined as:

$$S_{risk}^i = CS(x^i) * F(x^i) \tag{4}$$

where $CS(x^i)$ denotes the normalised consequence severity of the incident and $F(x^i)$ represents its relative occurrence frequency within the observed dataset. Eq. (4) defines risk as the product of incident frequency and consequence severity, reflecting the widely adopted view that risk is jointly determined by the likelihood of occurrence and the magnitude of consequences. Since S_{risk}^i is computed within the observed MCAD sample, it should be understood as a relative risk measure among reported maritime cyber incidents rather than an exposure-corrected absolute probability. The frequency term $F(x^i)$ therefore captures the relative prevalence of a scenario within the database, and the resulting risk levels are comparative rather than absolute in nature.

The consequence severity $CS(x^i)$ reflects the realised operational and safety impact of a cyber incident. Based on recorded outcomes in MCAD, severity is categorised into discrete levels and normalised to the interval [0, 1] to ensure comparability across incidents [54]:

$$CS(x^i) = \begin{cases} 0.33, & Consequence\ severity = Minor \\ 0.67, & Consequence\ severity = Moderate \\ 1, & Consequence\ severity = Major \end{cases} \tag{5}$$

Let A denote the occurrence of a cyberattack event, and B_t indicate the occurrence of an event belonging to a maritime cyberattack scenario $t (t \in T)$. Since a scenario t represents a specific case of maritime cyberattack, it follows that $B_t \subseteq A$. Under the assumption that $P(A) > 0$, the probability of observing scenario t can be expressed as:

$$P(B_t) = P(A)P(B_t|A) \tag{6}$$

The objective of this study is to evaluate and compare the relative risk structure of different attack scenarios conditional on the occurrence of a maritime cyberattack. Accordingly, the relative likelihood of each scenario is characterised by the conditional probability $P(B_t|A)$. Under this formulation, explicit estimation of $P(A)$ is not required, and the relative magnitudes of scenario probabilities remain directly comparable.

A frequency-based estimator is adopted to quantify $P(B_t|A)$, whereby the empirical conditional probability of each scenario is computed as the proportion of incidents assigned to that scenario. For an incident x^i belonging to a scenario t, the corresponding frequency term is defined as:

$$F(x^i) = P(B_t|A) = \frac{|C_t|}{N} \tag{7}$$

where $|C_t|$ denotes the number of incidents classified into scenario t and N represents the total number of incidents in the dataset. This formulation enables scenario-level aggregation of risk and supports comparative analysis across different categories of cyber threats.

To facilitate interpretation and subsequent analysis [54], the continuous risk score S_{risk}^i is discretised into ordinal risk levels. The

number of levels and cut-points is treated as an experimental design choice. A rank-based discretisation is adopted, in which risk levels are assigned according to the position of each incident within the empirical distribution of S^i_{risk}. Formally,

$$R^i = D\left(S^i_{risk}; L; q\right) \tag{8}$$

where L denotes the number of ordinal risk levels, $q = (q_1, \ldots, q_{L-1})$ denotes the empirical quantile cut-points, and D maps the continuous risk score to an ordinal risk level. Candidate 3-level and 5-level schemes, including equal-quantile and asymmetric quantile variants, are summarised in Table 2. This distribution-based ordinal classification provides a relative risk taxonomy for subsequent spatiotemporal and BN analyses.

3.4. Spatiotemporal risk mining

In maritime cybersecurity risk analysis, spatial heterogeneity and temporal evolution are critical for understanding how cyber threats concentrate, diffuse, and persist across regions. KDE [55] is adopted to transform discrete incident locations into a continuous spatial representation of risk intensity, thereby enabling identification of high-risk areas and potential diffusion patterns across geographical space.

Let X_{RIF} denotes the MCAD dataset, where each maritime cybersecurity incident x^i is associated with geographical coordinates $\left(lon^i, lat^i\right)$ and a corresponding quantitative risk score S^i_{risk}, as defined in Section 3.3. The KDE-based risk intensity at an arbitrary location (lon, lat) is expressed as:

$$\widehat{f}(lon, lat) = \frac{1}{m|H|^{\frac{1}{2}}} \sum_{i=1}^{m} S^i_{risk} K\left(H^{-\frac{1}{2}} \begin{bmatrix} lon - lon^i \\ lat - lat^i \end{bmatrix}\right) \tag{9}$$

where $K(\cdot)$ is a bivariate Gaussian kernel function and H denotes the bandwidth matrix. Weighting the kernel function by incident-specific risk scores allows both spatial proximity and within-sample relative risk magnitude to be jointly considered, producing a spatial density surface of relative risk among reported incidents [54].

Assuming approximate spatial isotropy and independence between longitude and latitude, the bandwidth matrix is specified using Scott's rule:

$$H = \begin{bmatrix} h^2 & 0 \\ 0 & h^2 \end{bmatrix}, h = m^{-\frac{1}{d+4}} \tag{10}$$

where d is the dimensionality of the spatial data, and $d = 2$ in this study.

To identify statistically significant spatial clustering of high-risk and low-risk areas, the Getis–Ord Gi* hotspot analysis [56] is applied. This method evaluates whether high or low values of risk are spatially concentrated beyond what would be expected under spatial randomness, thereby revealing localised clustering patterns. For a^{th} spatial unit, the Getis–Ord Gi* statistic is defined as:

$$G^*_a = \frac{\sum_{b=1}^{N} w_{ab} x_b - \overline{X} \sum_{b=1}^{N} w_{ab}}{S \sqrt{\frac{N \sum_{b=1}^{N} w_{ab}^2 - \left(\sum_{b=1}^{N} w_{ab}\right)^2}{N-1}}}$$
$$\overline{X} = \frac{1}{N} \sum_{b=1}^{N} x_b \tag{11}$$
$$S = \sqrt{\frac{\sum_{b=1}^{N} x_b^2}{N} - \overline{X}}$$

Here, x_b denotes the aggregated risk score of maritime cybersecurity incidents within spatial unit b, w_{ab} represents the spatial weight between units a and b, and N is the total number of spatial units. Spatial weights w_{ab} are constructed using a K-nearest neighbour (KNN) scheme to ensure consistent local neighbourhood definitions across heterogeneous spatial densities. The terms $\overline{X}$ and S indicate the mean and standard deviation of x_b, respectively. The statistic G^*_a approximately follows a standard normal distribution. Significantly positive values of G^*_a indicate high-risk hotspots, whereas significantly negative values correspond to low-risk cold spots, allowing spatial risk concentrations to be quantitatively identified and compared.

To further capture the temporal evolution of spatial risk patterns, the study period is divided into four periods:

(1) Period I (2010–2014): early deployment of networked maritime infrastructure;
(2) Period II (2015–2019): acceleration of system interconnection and digitalisation;
(3) Period III (2020–2022): rapid digitalisation, remote operations, and increased cyber exposure;
(4) Period IV (2023–2025): development of intelligent shipping and strengthened cybersecurity awareness.

For each period, KDE is applied to generate a period-specific continuous risk intensity surface, followed by Getis–Ord Gi* analysis to identify statistically significant hotspots and cold spots. This combined spatiotemporal approach enables quantitative comparison of risk concentration, diffusion, and persistence across different developmental stages of the maritime system, providing empirical evidence for region-specific risk mitigation and adaptive cybersecurity strategies.

3.5. BN-based analysis

To represent temporal dynamics within the BN framework, time is incorporated as a RIF through a categorical variable derived from calendar year. Maritime cyber incidents are classified into four temporal periods: 2010–2014, 2015–2019, 2020–2022, and 2023–2025. This temporal classification is aligned with the four-period scheme adopted in Section 3.4 for spatiotemporal analysis. The segmentation facilitates the identification of recent changes in the relationships among RIFs and risk levels during the period of intensified maritime cyber activity.

In information-theoretic risk modelling, information entropy quantifies the uncertainty associated with a random variable. In this study,

Table 2
Binning schemes for five-level and three-level risk labels.

Level	Type	bins	labels
3-level-	equal	[0, 0.333, 0.667, 1.0]	['Low', 'Medium', 'High']
3-level-	high-wide	[0, 0.2, 0.5, 1.0]	['Low', 'Medium', 'High']
3-level-	low-wide	[0, 0.4, 0.7, 1.0]	['Low', 'Medium', 'High']
3-level-	symmetric	[0, 0.25, 0.55, 1.0]	['Low', 'Medium', 'High']
5-level-	equal	[0, 0.2, 0.4, 0.6, 0.8, 1.0]	['Very low', 'Low', 'Medium', 'High', 'Very high']
5-level-	low-wide	[0, 0.3, 0.55, 0.75, 0.9, 1.0]	['Very low', 'Low', 'Medium', 'High', 'Very high']
5-level-	high-wide	[0, 0.1, 0.25, 0.45, 0.7, 1.0]	['Very low', 'Low', 'Medium', 'High', 'Very high']
5-level-	symmetric	[0, 0.15, 0.35, 0.6, 0.85, 1.0]	['Very low', 'Low', 'Medium', 'High', 'Very high']

each RIF is modelled as a discrete random variable RIF_i with a probability distribution $p(x)$. The entropy of RIF_i is defined as:

$$H(RIF_i) = -\sum_{x \in RIF_i} p(x)\log p(x) \tag{12}$$

which measures the intrinsic uncertainty and information content of the factor.

To examine the influence of RIFs on maritime cybersecurity risk levels, MI is used to quantify the statistical dependence between each RIF_i and risk level (R), without imposing parametric assumptions regarding their relationship. The MI between RIF_i and R is expressed as:

$$I(RIF_i; R) = H(RIF_i) + H(R) - H(RIF_i, R) \tag{13}$$

where larger values indicate stronger statistical dependence.

Conventional Naïve Bayes classifiers assume conditional independence among RIFs given the risk level (R). In maritime cybersecurity applications, however, RIFs are often interrelated due to common system architectures, attack vectors, and operational conditions, rendering this assumption unrealistic. To capture these dependencies, a TAN model is employed. TAN relaxes the strict independence assumption by allowing each RIF to depend on both the target variable (R) and one additional RIF, thereby forming a tree-structured BN. This structure enables the model to represent key inter-factor dependencies while maintaining computational tractability and predictive efficiency.

The network structure is learned by constructing a maximum-weight spanning tree, where edge weights are defined by conditional mutual information $I(RIF_i; RIF_j|R)$. The resulting joint probability distribution is given by:

$$P(R, RIF_1, RIF_2, \ldots, RIF_n) = P(R)\prod_{i=1}^{n} P(RIF_i|R, Pa(RIF_i)) \tag{14}$$

where $Pa(RIF_i)$ denotes the parent of RIF_i in the learned tree structure.

The TAN model provides an interpretable, data-driven approach to maritime cybersecurity risk assessment by accounting for probabilistic dependencies among RIFs. It supports dependency-aware risk analysis, probabilistic inference, and the prediction of high-risk cybersecurity scenarios. However, the directed edges in the TAN represent statistical dependencies used to factorise the joint probability distribution and should not be interpreted as causal relationships.

4. Experimental results and analysis

4.1. Data description

The empirical analysis draws on the MCAD, which contains 447 documented maritime cyber incidents. Only three incidents were recorded before 2010. Given the limited representation of this period, the analysis focuses on the 444 incidents recorded from 2010 onwards. The descriptive statistics for the selected RIFs are presented in Table 3.

The annual distribution of reported incidents is uneven, with a marked concentration after 2020. The geographical attribution of attacks remains uncertain, as the attacking country is unknown for a substantial proportion of incidents. Among those with identified origins, Russia Federation, China, North Korea and Iran feature prominently. Most recorded incidents are classified as intentional and externally initiated, suggesting that deliberate external attacks account for the majority of cases documented in MCAD.

Shipping companies, vessels and ports are the most frequently reported targets. Ransomware accounts for the largest share of recorded cyber threats, followed by spoofing, hacking, distributed denial-of-service (DDoS) attacks, malware, jamming and phishing. Among incidents with identifiable victim countries, the United States, China, the United Kingdom, Russia Federation, Republic of Korea, France and Australia are frequently represented. However, the substantial number of unknown or broadly classified victim locations limits the geographical interpretation of these records. Network and hardware systems are the most commonly exploited assets, followed by media and data resources and application and software systems.

Table 3
RIF description.

RIF	Description and probability
Year	2010–2014 (4.3%), 2015–2019 (16.0%), 2020–2022 (31.7%), 2023–2025 (48.0%)
Attack countries	Unknown (46.8%), Russia Federation(32.2%), Others (7.2%), China (6.8%), North Korea (3.6%), Iran (3.4%)
Victim countries	Others (36.9%), Unknown (35.1%), United States (9.9%), China (3.6%), United Kingdom (3.4%), Russia Federation (3.2%), Republic of Korea(2.9%), France (2.7%), Australia (2.3%)
Target	Other (28.6%), Shipping company (24.1%), Vessel (20.5%), Port (14.0%), Shipbuilding firm (9.2%), Energy distributor (3.6%)
Cyber threats	Ransomware (53.4%), Spoofing (15.8%), Hacking (12.4%). DDoS (5.6%), Malware (5.6%), Jamming (5.2%), Phishing (2.0%)
Consequence severity	Moderate (70.0%), Minor (25.5%), Major (4.5%)
Intent	Intentional (99.3%), Unintentional (0.7%)
Origin	External (98.4%), Internal (1.6%)
Asset exploited	Network (34.7%), Hardware (22.7%), Media/Data (20.5%), Application/Software (18.5%), People/Processes (2.7%), Other (0.9%)
Consequence type	Business Disruption (56.5%), Manipulation of Maritime Information (20.1%), Data Breach (18.0%), Other (4.7%), Theft or Loss of Funds or Cargoes (0.7%)

Business disruption is the most frequently reported consequence, followed by manipulation of maritime information and data breaches. Most incidents are classified as having moderate severity, while minor and major consequences account for smaller proportions. Although major-severity incidents are less frequent, their potential to disrupt critical maritime functions warrants particular attention in risk assessment. These descriptive patterns provide the empirical basis for the subsequent analysis of cyberattack scenarios, spatiotemporal risk patterns and dependencies among RIFs.

4.2. Cluster analysis of cyber attack events

The optimal number of clusters was determined by comparing multiple categorical clustering approaches. K-modes [57], agglomerative hierarchical clustering [58], LCA [53], and ROCK (Robust Clustering using LinKs) [59] were evaluated for $k = 4$ to 9 using the silhouette score. As shown in Table 4, ROCK performed poorly on this dataset, with negative silhouette values for most k, while agglomerative clustering and K-modes showed relatively flat performance. LCA achieved the highest silhouette score at $k = 5$ (0.146), marginally above $k = 4$ (0.145). Considering statistical quality, class size balance, and scenario interpretability, LCA with $k = 5$ was selected as the final clustering solution.

The within-class distributions of RIFs for the five LCA latent classes are summarised in Table 4. Based on these dominant characteristics, the maritime cyber incidents are categorised into five distinct cyberattack scenarios.

To identify the attributes that distinguish each latent class, two criteria were applied to the conditional distributions of the RIFs. Within-

Table 4
Silhouette scores of different clustering algorithms across $k = 4$–9.

Algorithm	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$	$k=9$
Agglomerative	0.108	0.101	0.108	0.1	0.101	0.085
K-modes	0.097	0.106	0.108	0.104	0.092	0.097
LCA	0.145	**0.146**	0.128	0.105	0.109	0.117
ROCK	0.012	0.015	−0.049	−0.047	−0.053	−0.059

Table 5
Risk factor distribution for each cluster category.

RIF		Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5
Asset exploited	Application/Software	30.6%	0.0%	0.0%	**50.0%**	20.4%
	Hardware	0.0%	**97.9%**	0.0%	17.6%	0.0%
	Media/Data	0.0%	0.0%	46.7%	0.0%	36.5%
	Network	**69.4%**	0.0%	53.3%	0.0%	41.7%
	Other	0.0%	0.0%	0.0%	2.9%	1.4%
	People/Processes	0.0%	2.1%	0.0%	29.4%	0.0%
Attack countries	China	1.4%	13.4%	16.7%	32.4%	0.0%
	Iran	6.9%	8.2%	0.0%	5.9%	0.0%
	North Korea	0.0%	12.4%	10.0%	2.9%	0.0%
	Other	12.5%	13.4%	6.7%	20.6%	0.5%
	Russian Federation	33.3%	21.6%	6.7%	0.0%	45.5%
	Unknown	45.8%	30.9%	**60.0%**	38.2%	54.0%
Consequence severity	Major	5.6%	6.2%	3.3%	0.0%	4.3%
	Minor	30.6%	45.4%	43.3%	50.0%	8.1%
	Moderate	63.9%	48.5%	53.3%	50.0%	**87.7%**
Consequence type	Business Disruption	**100.0%**	7.2%	13.3%	11.8%	77.7%
	Data Breach	0.0%	0.0%	43.3%	**58.8%**	22.3%
	Manipulation of Maritime Information	0.0%	**90.7%**	0.0%	2.9%	0.0%
	Other	0.0%	2.1%	**43.3%**	17.6%	0.0%
	Theft or Loss of Funds or Cargoes	0.0%	0.0%	0.0%	8.8%	0.0%
Cyber threats	DDoS	**33.3%**	0.0%	0.0%	2.9%	0.0%
	Hacking	11.1%	3.1%	**100.0%**	41.2%	0.0%
	Jamming	0.0%	23.7%	0.0%	0.0%	0.0%
	Malware	23.6%	0.0%	0.0%	23.5%	0.0%
	Phishing	0.0%	0.0%	0.0%	26.5%	0.0%
	Ransomware	31.9%	2.1%	0.0%	2.9%	**100.0%**
	Spoofing	0.0%	**71.1%**	0.0%	2.9%	0.0%
Intent	Intentional	100.0%	97.9%	96.7%	100.0%	100.0%
	Unintentional	0.0%	2.1%	3.3%	0.0%	0.0%
Origin	External	100.0%	92.8%	100.0%	100.0%	100.0%
	Internal	0.0%	7.2%	0.0%	0.0%	0.0%
Target	Energy distributor	2.8%	0.0%	3.3%	0.0%	6.2%
	Other	16.7%	12.4%	**43.3%**	26.5%	38.4%
	Port	**63.9%**	1.0%	0.0%	11.8%	5.2%
	Shipbuilding firm	4.2%	1.0%	33.3%	5.9%	11.8%
	Shipping company	11.1%	0.0%	20.0%	35.3%	**38.4%**
	Vessel	1.4%	**85.6%**	0.0%	20.6%	0.0%
Victim countries	Australia	2.8%	1.0%	0.0%	5.9%	2.4%
	China	0.0%	10.3%	0.0%	11.8%	0.9%
	France	4.2%	0.0%	10.0%	0.0%	2.8%
	Other	**65.3%**	32.0%	30.0%	26.5%	32.2%
	Republic Of Korea	2.8%	6.2%	13.3%	0.0%	0.5%
	Russian Federation	1.4%	10.3%	3.3%	5.9%	0.0%
	United Kingdom	5.6%	3.1%	6.7%	2.9%	2.4%
	United States	16.7%	5.2%	13.3%	8.8%	9.5%
	Unknown	1.4%	32.0%	23.3%	38.2%	**49.3%**
Summary	Event Count	72	97	30	34	211
	Event %	16.2%	21.8%	6.8%	7.7%	47.5%

cluster dominance identifies the most prevalent category of a given RIF within a cluster, whereas cross-cluster maximum identifies the cluster in which a particular category has its highest proportion. The former describes the typical characteristics of a cluster, while the latter helps distinguish it from other clusters. Attributes meeting both criteria are highlighted in bold in Table 5 and used to interpret and label the five LCA-derived cyberattack scenarios.

(1) Port-targeted network disruption and business interruption (Cluster 1). This cluster is characterised by port targets, network assets, DDoS attacks and business disruption, all of which meet both criteria. The Other category also has the highest cross-cluster proportion among victim countries. Attack countries are predominantly unknown, and most incidents are classified as having moderate consequences. DDoS and malware are the principal reported threats. The cluster represents cyber incidents affecting port networks and associated operations, where disruption to interconnected digital systems can interrupt port services and business activities.
(2) Maritime information spoofing against vessel hardware (Cluster 2). Vessel targets, hardware assets, spoofing attacks and manipulation of maritime information are the defining attributes of this cluster. Iran and North Korea have relatively high proportions among the identified attack countries, while major-severity incidents have their highest cross-cluster representation in this group. The scenario primarily concerns spoofing and jamming attacks affecting shipboard systems and maritime information. Such incidents may compromise the integrity of navigational information and create safety-related risks.
(3) Hacking-driven cyber intrusion and data breach (Cluster 3). This cluster is distinguished by hacking attacks, unknown attack countries, and the Other categories for both targets and consequences. Media and data assets have their highest cross-cluster proportion in this group, as do France, the Republic of Korea and the United Kingdom among victim countries. The incidents mainly involve hacking-related intrusions affecting shipbuilding firms and other maritime organisations, with consequences including data breaches and outcomes not covered by the specified consequence categories. The prevalence of unspecified attributes also limits the precision with which this scenario can be characterised.

(4) Phishing/hacking-driven data breach targeting shipping companies (Cluster 4). Application and software assets and data breaches are the principal distinguishing attributes of this cluster. Phishing has its highest cross-cluster proportion, although hacking is the most prevalent threat within the cluster. Shipping companies are the main targets, while China and Australia have the highest cross-cluster proportions among victim countries. The incidents primarily involve attacks on application and software systems, resulting in data breaches and, in some cases, financial losses or the loss of cargo-related assets.
(5) Ransomware-driven business disruption (Cluster 5). This cluster is characterised by ransomware attacks, shipping company targets, moderate consequence severity and unknown victim countries. The Russian Federation has the highest cross-cluster proportion among identified attack countries, while business disruption is the predominant consequence. Cluster 5 contains the largest number of incidents and represents ransomware attacks that interrupt shipping company operations and associated business processes.

The distribution of incidents across the five clusters shows that ransomware-driven business disruption is the most frequently recorded scenario in MCAD. The other clusters account for smaller proportions but involve different combinations of targets, threats and consequences. In particular, port network disruption and vessel information spoofing concern systems relevant to operational continuity and navigational safety, while hacking- and phishing-related scenarios primarily affect organisational data and software assets. These distinctions are important because incident frequency alone does not capture differences in consequence severity.

To examine the contribution of each scenario to the overall risk measure, the five clusters were evaluated using the frequency–severity formulation introduced in Section 3.3. Scenario frequency was calculated as the proportion of incidents assigned to each cluster. Mean severity was obtained by weighting the proportions of minor, moderate and major incidents within each cluster by their respective severity weights. The relative risk of each scenario was then calculated as the product of its frequency and mean severity. Finally, each scenario's risk share was obtained by dividing its relative risk by the sum of the relative risks across all five clusters. The results are reported in Table 6.

Cluster 5 makes the largest contribution to the aggregated relative risk, accounting for 52.2%, compared with 47.5% of the recorded incidents. This difference reflects its mean severity of 0.657, which exceeds the frequency-weighted sample average of 0.598. Cluster 2 ranks second, contributing 19.6% of the relative risk from 21.8% of incidents. Cluster 1 has a mean severity of 0.584, but its lower incident frequency (16.2%) limits its risk share to 15.9%. Clusters 3 and 4 contribute 6.0% and 6.4%, respectively, primarily because they account for smaller proportions of the recorded incidents.

These results show that the contribution of each scenario depends on both its occurrence frequency and its consequence severity. Ransomware-driven business disruption contributes the largest share because of its high frequency and above-average severity. Maritime information spoofing also makes a substantial contribution, partly reflecting the greater proportion of major-severity incidents within that cluster. The remaining scenarios contribute less to the aggregated risk measure, although their consequences may still be significant for particular maritime systems and operations.

Table 6
Scenario-level frequency–severity decomposition.

Scenario	Incidents	Frequency	Mean severity	Relative risk	Rank
C1	72	16.20%	0.584	0.095	3
C2	97	21.80%	0.536	0.117	2
C3	30	6.80%	0.534	0.036	5
C4	34	7.70%	0.5	0.038	4
C5	211	47.50%	0.657	0.312	1
Total	444	100.00%	0.598	0.598	-

The five scenarios therefore provide a classification of the incident patterns recorded in MCAD, while the frequency–severity analysis distinguishes their relative contributions to the dataset-based risk measure. This classification is used in the subsequent spatiotemporal analysis and TAN-based modelling of dependencies among RIFs.

4.3. Quantitative spatiotemporal analysis of cyber attack incident risk

Relative risk intensity measures derived from scenario-based clustering and consequence severity enable a joint spatiotemporal examination of reported maritime cyber incidents in the MCAD. This analysis identifies periods of relative risk escalation and geographically concentrated hotspots among reported incidents, providing a quantitative foundation for early warning, emergency-response planning, and risk-informed policy intervention.

4.3.1. Temporal risk analysis

Fig. 2 shows the annual distribution of reported maritime cyber incidents across the three relative risk levels from 2010 to 2025. The number of recorded incidents increases from the mid-2010s onwards, accompanied by a growing number of incidents classified as medium or high risk. The period 2018–2020 shows a more sustained concentration of higher-risk incidents than the preceding years.

This pattern becomes more pronounced during 2021–2025. High-risk incidents increase notably in 2022 and reach their highest recorded levels in 2023, exceeding 50 incidents in the peak year. The distribution also indicates a greater representation of medium- and high-risk incidents in the later years of the study period.

These findings suggest that higher-scoring incidents have become more prominent in the MCAD records over time. However, the observed increase may also reflect changes in reporting coverage, incident detection and database completeness. Without consistent measures of maritime cyber exposure, the results cannot establish a corresponding increase in the underlying incidence rate or absolute risk. The temporal patterns should therefore be interpreted as changes in the frequency and relative risk composition of reported incidents, rather than evidence of a system-wide escalation in maritime cyber risk.

4.3.2. Spatial risk distribution and hotspot analysis

KDE and Getis–Ord hotspot analysis are employed to visualise the spatial distribution and clustering of maritime cybersecurity incidents from 2010 to 2025. Fig. 3 and Fig. 4 illustrate the global risk intensity surface and statistically significant clustering patterns, respectively.

According to the KDE results (Fig. 3), relative risk of reported maritime cyber incidents exhibit strong spatial concentration at the global scale, with high-intensity zones primarily distributed along the coastlines of Europe, North America, and East Asia. Europe displays the highest overall risk density, with continuous clusters spanning the North Sea, Baltic Sea, and Mediterranean regions. Major ports in the United Kingdom, the Netherlands, and Germany emerge as dominant risk nodes, reflecting advanced digitalisation, dense port networks, and high operational connectivity, all of which expand the cyberattack surface. North America represents the second-highest concentration, characterised by highly interconnected port infrastructures and extensive information exposure. East Asia also demonstrates distinct clustering patterns, consistent with the rapid adoption of smart vessels, automated terminals, and intelligent port systems, accompanied by rising cyber risk. Overall, the spatial distribution closely aligns with global shipping intensity, digital maturity, and geo-economic centrality, resulting in pronounced coastal concentration and node-centric aggregation of cyber risk.

The hotspot analysis (Fig. 4) further corroborates these spatial patterns. High-confidence hotspots are primarily concentrated along the

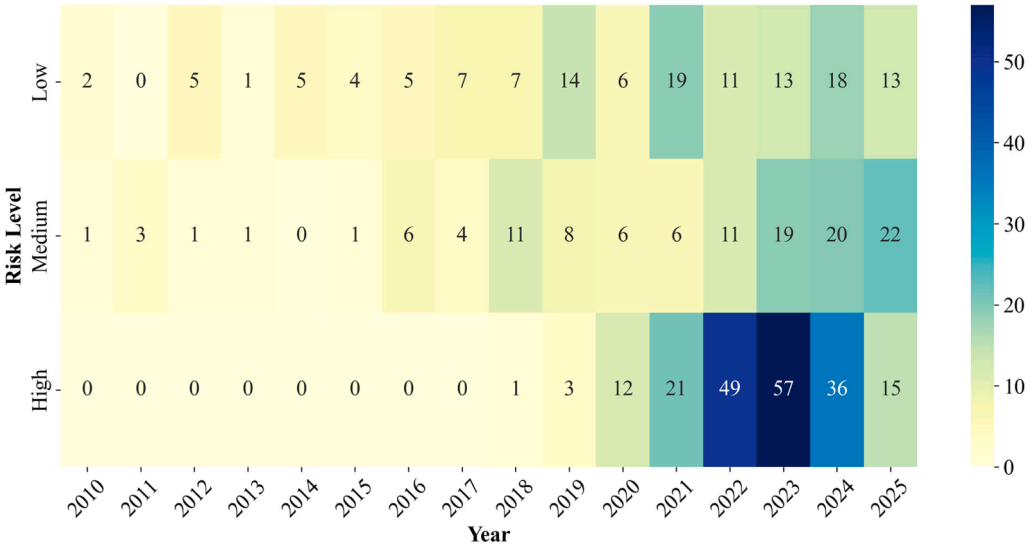


Fig. 2. Evolution of Cyber Attack Risks.

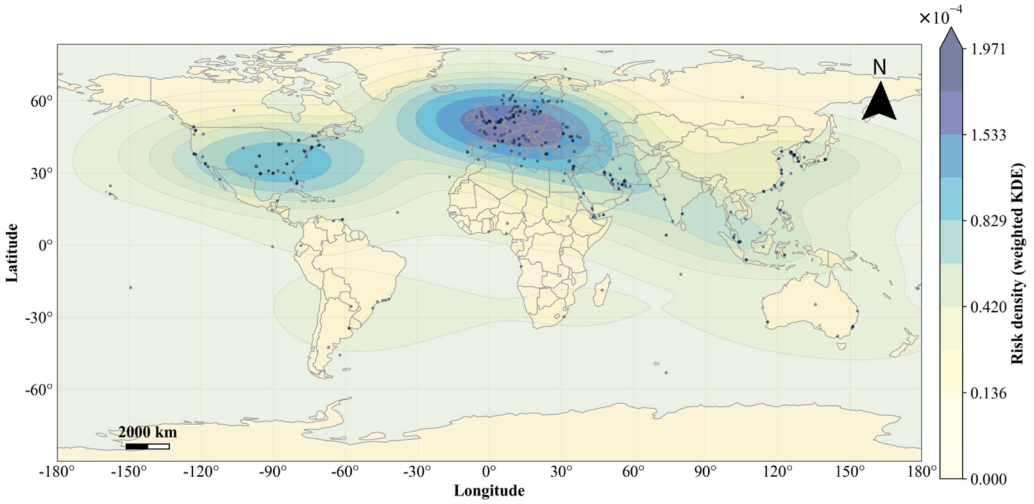


Fig. 3. KDE visualisation of Cyber attack events.

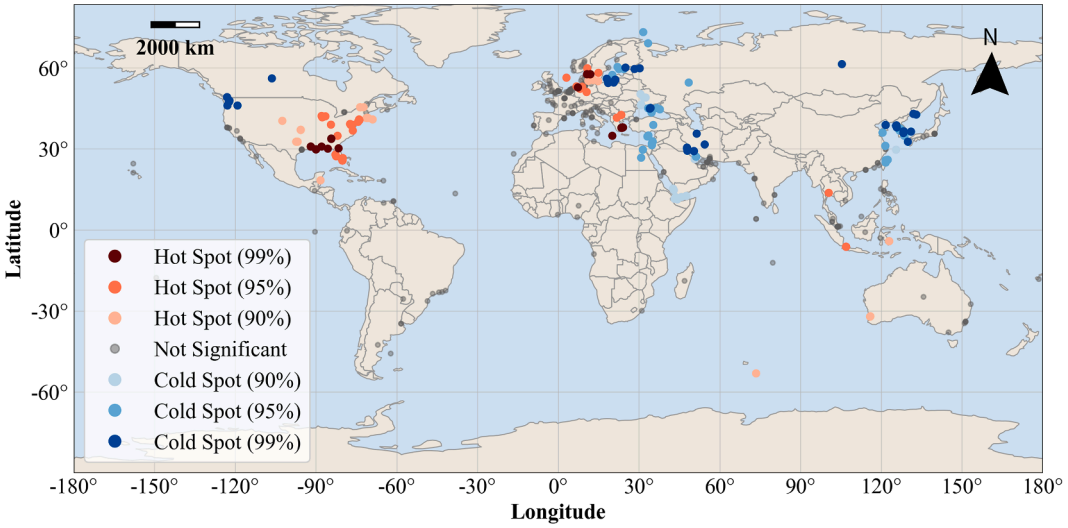


Fig. 4. Hot spot analysis results.

coastlines of Europe, North America, and Southeast Asia. At the 99% confidence level, Europe and the eastern coast of North America exhibit the most extensive hotspot coverage, with core areas centered around major maritime hubs in Europe and the United States, indicating a relatively higher level of risk within the MCAD dataset. At the 95% confidence level, multiple hotspots appear across North America and Europe, suggesting that risks may spill over between interconnected port systems. The emergence of hotspots in Southeast Asia may reflect accelerating accumulation of cyber risks, driven by the expansion of international shipping and the advancement of port automation. In contrast, cold spots are mainly identified in regions such as Central Asia and Northeast Asia, indicating a relative lower concentration of recorded cybersecurity incidents compared with Europe and the North America.

Taken together, the spatiotemporal analyses reveal pronounced coastal concentration, regional disparities, and dynamic escalation of maritime cyber risk. These findings provide empirical support for zonal defence strategies, prioritised cybersecurity investment, and adaptive international governance mechanisms, contributing to enhanced resilience and safety of global maritime systems.

4.3.3. Spatiotemporal analysis

Figs. 5 and 6 show the spatial distribution of reported maritime cyber incidents between 2010 and 2025, using KDE and Getis–Ord Gi* hotspot analysis, respectively. The results are examined across four periods to assess changes in incident density, geographical concentration and statistically significant spatial clustering.

(1) 2010–2014: Emergence phase ($n = 19$)

Only 19 incidents were recorded during this period, with no well-established pattern of spatial clustering. The KDE results (Fig. 5a) show small, localised concentrations in parts of East Asia, alongside scattered incidents in North America and Europe. The hotspot analysis (Fig. 6a) identifies a limited number of cold spots in the Middle East, but no significant hotspots. Given the small sample size, these results provide limited evidence of the geographical distribution of maritime cyber threats during this period.

(2) 2015–2019: Regional clustering phase ($n = 71$)

The number of recorded incidents increased to 71, accompanied by more distinct regional concentrations. The KDE results (Fig. 5b) indicate higher incident densities in East Asia and Europe. The Getis–Ord Gi* analysis (Fig. 6b) identifies scattered hotspots at the 90% confidence level in parts of North America and East Asia. These findings suggest that reported incidents were becoming more geographically concentrated, although the identified hotspots remained relatively limited in extent. This period also coincided with increasing digitalisation and connectivity in maritime operations, which may have expanded exposure to cyber threats.

(3) 2020–2022: Multicentre clustering phase ($n = 141$)

Between 2020 and 2022, the number of recorded incidents increased to 141, and the spatial distribution became more dispersed across several major maritime regions. The KDE results (Fig. 5c) show distinct concentrations in Europe, North America, and East and Southeast Asia. The hotspot analysis (Fig. 6c) identifies statistically significant hotspots at the 95% confidence level, particularly in Europe. Compared with the preceding period, the results indicate a shift towards multiple regional concentrations rather than clustering around a small number of locations.

(4) 2023–2025: Expansion of regional concentrations ($n = 213$)

The most recent period accounts for 213 recorded incidents, the largest number among the four periods. The KDE results (Fig. 5d) show extensive areas of elevated incident density across North America, Europe and the Asia-Pacific region. The hotspot analysis (Fig. 6d) identifies a wider distribution of hotspots at the 95% confidence level, including the eastern coast of North America, major European maritime centres, and coastal areas of Southeast Asia. These results indicate that the geographical concentration of reported incidents has become more widespread, with statistically significant clustering observed across several maritime regions.

Overall, the spatial analyses indicate a progression from scattered incidents in 2010–2014 to more extensive regional concentrations during 2023–2025. The KDE results show increasing densities of reported incidents, while the Getis–Ord Gi* analysis identifies changes in the location and extent of statistically significant clusters. By the final period, hotspots are distributed across several major maritime regions, particularly North America, Europe, and East and Southeast Asia.

These patterns suggest that maritime cyber incidents are not evenly distributed geographically and that their spatial concentration has changed over time. However, the increase in recorded incidents may also reflect changes in reporting practises and database coverage. Furthermore, the apparent association between incident concentrations and major maritime centres does not establish a causal relationship with shipping activity or port digitalisation. The findings nevertheless provide a geographical basis for examining where reported cyber incidents are concentrated and for considering regional differences in maritime cybersecurity risk.

4.4. BN analysis of cyber attack risk

4.4.1. MI analysis

Fig. 7 presents the MI between individual RIFs and the assigned risk levels. Cyber Threats exhibits the highest MI (0.530), followed by Asset Exploited (0.231), Target (0.216), Year (0.166) and Attack Countries (0.160). These variables provide the most information about risk-level differences within the MCAD sample. In contrast, Victim Countries (0.068), Origin (0.009) and Intent (0.004) show relatively weak associations with risk level. The low MI values for Origin and Intent may partly reflect their highly imbalanced distributions. Overall, the results indicate that cyber threat type, exploited asset and target category are the most informative RIFs for distinguishing the assigned risk levels. These associations are descriptive and should not be interpreted as evidence of causal effects.

4.4.2. TAN analysis

Fig. 8 presents the final TAN model for maritime cyberattack risk analysis [60,61]. To reduce target leakage, Consequence Severity and Consequence Type were excluded from the predictor set, as these variables are directly or closely related to the construction of the risk labels. The remaining RIFs are connected to the Risk Level node, with

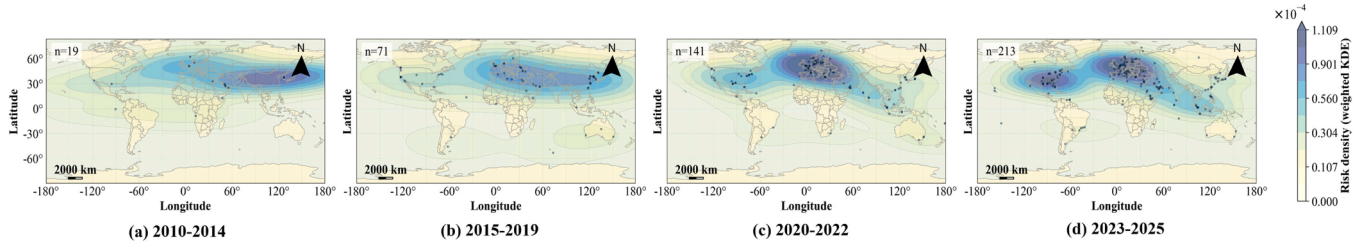


Fig. 5. KDE analysis of cyber attack time evolution.

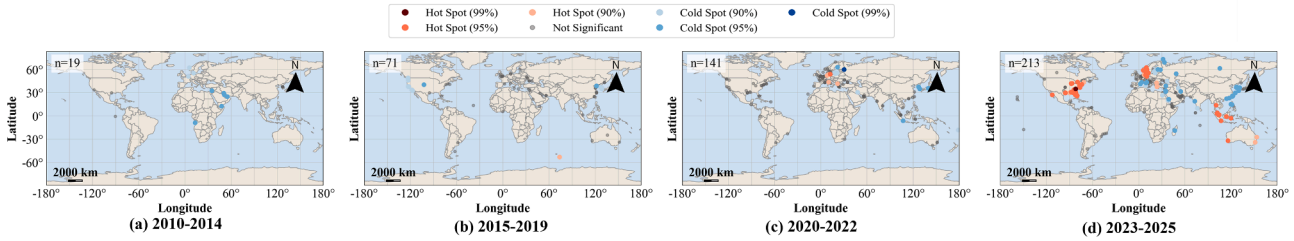


Fig. 6. Getis–Ord Gi* analysis of time evolution of cyber attacks.

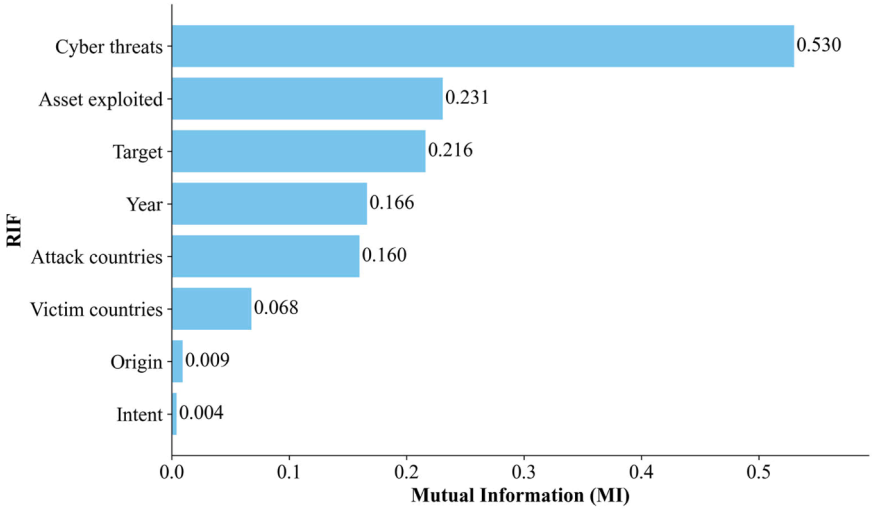


Fig. 7. MI visualisation.

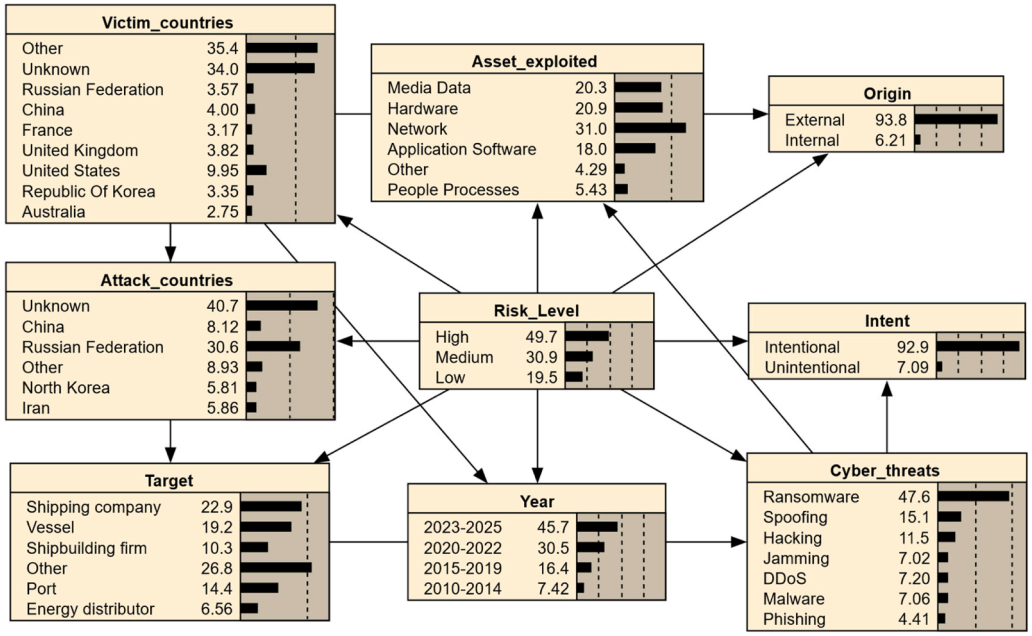


Fig. 8. The constructed TAN model for maritime cyber attack.

additional edges representing conditional dependencies between predictors. These directed edges describe the factorisation of the joint probability distribution and should not be interpreted as causal relationships.

The TAN model was evaluated using stratified fivefold cross-validation. We compared four risk-level partitioning schemes (equal-width, high-wide, low-wide and symmetric), each with three and five risk levels. We also examined the effect of including or excluding Intent and Origin, whose distributions are highly imbalanced and whose mutual information with risk level is low.

As shown in Table 7, the three-level classifications generally achieved higher F1-scores than the five-level alternatives. The best performance was obtained using the three-level high-wide scheme with Intent and Origin retained, yielding an accuracy of 0.874 ± 0.052 and an F1-

score of 0.849 ± 0.065. Removing these two variables reduced accuracy slightly to 0.865 ± 0.061 and the F1-score to 0.838 ± 0.076. Their inclusion therefore provides a modest improvement in classification performance, although their low mutual information indicates limited individual discriminatory value within the MCAD sample.

The three-level high-wide configuration was consequently selected for the final TAN model. The model provides a means of examining conditional associations between incident characteristics and the assigned risk levels. Its results should be interpreted as within-sample probabilistic relationships rather than causal explanations or independently validated estimates of maritime cyber risk.

4.4.3. Scenario 1: attacker-condition-driven risk patterns

This scenario examines the probability of an assigned high-risk level under a specified combination of incident characteristics. The evidence variables include Target, Intent, Origin, Attack Countries, Year and Cyber Threats.

As shown in Fig. 9, the configuration comprises shipping companies as the target, intentional and externally originated attacks, an unknown attack country, incidents recorded during 2023–2025, and ransomware as the cyber threat. Given this evidence, the TAN model estimates a 99.2% conditional probability of High risk. This is substantially higher than the overall proportion of high-risk incidents in the analysed sample.

The result indicates a strong modelled association between this combination of recorded characteristics and the assigned high-risk category. Ransomware and the targeting of shipping companies are prominent features of the configuration. However, Attack Countries = Unknown denotes incomplete geographical attribution rather than a distinct attacker characteristic. The estimated probability should therefore be interpreted as a conditional prediction within the MCAD-based model, not as evidence of a specific attacker profile or the causal effects of individual factors.

4.4.4. Scenario 2: victim-condition-driven risk patterns

Scenario 2 examines the assigned risk level under a combination of victim-related and exploited-asset characteristics. As illustrated in Fig. 10, the selected evidence includes Victim Countries = Others, Asset Exploited = Media/Data and the period 2023–2025. The TAN model estimates an 87.3% conditional probability of High risk for this configuration.

The result suggests that incidents recorded under these conditions are strongly associated with the high-risk category in the fitted model. Media/Data represents the exploited asset category, while Others is an aggregated geographical classification and should not be interpreted as a specific national risk factor. The estimate does not establish that data assets or particular victim locations independently increase cyber risk. Rather, it illustrates how the TAN model combines recorded incident characteristics to estimate the probability of an assigned risk level.

4.4.5. Scenario 3: reverse analysis from risk level to RIF

To examine the incident characteristics associated with the high-risk category, the TAN model was conditioned on Risk Level = High. Fig. 11 presents the resulting posterior distributions of the RIFs.

Ransomware accounts for 83.4% of the posterior distribution of Cyber Threats. For Asset Exploited, the Network and Application/Software categories account for 37.4% and 19.4%, respectively. Shipping companies (33.8%) and Others (34.8%) are prominent target categories. In the Attack Countries distribution, Unknown accounts for 48.3%, while the Russian Federation represents 40.9%. For Victim Countries, the United States and the United Kingdom account for 9.13% and 3.48%, respectively.

These distributions describe the relative prevalence of recorded characteristics conditional on the modelled high-risk category. They do not represent the probability that an incident involving a particular country, target or asset will be classified as high risk. In particular, the substantial Unknown category reflects incomplete attribution, and the posterior share associated with a named country should not be interpreted as verified responsibility for cyberattacks.

The reverse inference complements the preceding analyses by characterising the incident attributes most frequently associated with the high-risk state in the fitted TAN model. The prominence of ransomware and network-related exploited assets is consistent with the scenario-level findings, while the attribution results highlight an important limitation of the available records. These associations provide a descriptive basis for further investigation rather than evidence of causal mechanisms or attack propagation.

5. Discussion and implications

5.1. Discussion

The results reveal substantial differences in the frequency, severity and geographical distribution of reported maritime cyber incidents. These differences have implications for how incident-based risk estimates are interpreted. In particular, the findings show that incident counts alone do not adequately represent the relative importance of different attack scenarios, while geographical concentrations and statistical dependencies provide complementary information that cannot be obtained from frequency–severity scores alone.

Table 7
Ablation study on intent and origin across risk-level binning schemes.

With RIF	Risk level	Type	Accuracy	Precision	Recall	F1
With intent origin	**3-level**	equal	0.777±0.061 [0.702,0.852]	0.755±0.065 [0.674,0.836]	0.738±0.064 [0.659,0.818]	0.736±0.066 [0.655,0.818]
		high-wide	**0.874±0.052 [0.810,0.938]**	**0.856±0.069 [0.771,0.941]**	**0.845±0.064 [0.766,0.924]**	**0.849±0.065 [0.768,0.930]**
		low-wide	0.797±0.042 [0.745,0.849]	0.716±0.066 [0.634,0.797]	0.698±0.061 [0.622,0.773]	0.694±0.065 [0.614,0.774]
		symmetric	0.786±0.026 [0.754,0.818]	0.760±0.045 [0.704,0.816]	0.748±0.037 [0.702,0.794]	0.750±0.040 [0.701,0.800]
	5-level	equal	0.723±0.016 [0.703,0.743]	0.549±0.031 [0.511,0.588]	0.527±0.019 [0.503,0.551]	0.526±0.017 [0.506,0.547]
		high-wide	0.703±0.039 [0.655,0.750]	0.666±0.063 [0.588,0.744]	0.597±0.048 [0.537,0.656]	0.614±0.054 [0.547,0.681]
		low-wide	0.754±0.042 [0.702,0.807]	0.435±0.036 [0.390,0.480]	0.445±0.033 [0.404,0.487]	0.438±0.034 [0.396,0.481]
		symmetric	0.750±0.023 [0.721,0.779]	0.584±0.026 [0.552,0.616]	0.562±0.011 [0.549,0.576]	0.564±0.014 [0.547,0.581]
Without intent origin	3-level	equal	0.777±0.061 [0.702,0.852]	0.755±0.065 [0.674,0.836]	0.738±0.064 [0.659,0.818]	0.736±0.066 [0.655,0.818]
		high-wide	0.865±0.061 [0.789,0.941]	0.847±0.079 [0.749,0.944]	0.835±0.074 [0.743,0.927]	0.838±0.076 [0.744,0.933]
		low-wide	0.811±0.048 [0.751,0.871]	0.757±0.071 [0.668,0.845]	0.727±0.054 [0.659,0.794]	0.731±0.058 [0.658,0.803]
		symmetric	0.784±0.030 [0.747,0.821]	0.757±0.048 [0.697,0.817]	0.745±0.042 [0.693,0.797]	0.747±0.045 [0.692,0.802]
	5-level	equal	0.723±0.028 [0.689,0.757]	0.546±0.031 [0.507,0.585]	0.526±0.026 [0.493,0.558]	0.526±0.025 [0.494,0.557]
		high-wide	0.716±0.038 [0.668,0.764]	0.680±0.059 [0.607,0.754]	0.617±0.046 [0.559,0.675]	0.631±0.055 [0.563,0.699]
		low-wide	0.754±0.044 [0.700,0.809]	0.436±0.038 [0.389,0.483]	0.445±0.034 [0.403,0.488]	0.438±0.035 [0.395,0.482]
		symmetric	0.761±0.016 [0.742,0.781]	0.596±0.010 [0.583,0.609]	0.567±0.009 [0.556,0.578]	0.572±0.006 [0.564,0.580]

Note: Values are mean ± SD across stratified 5-fold cross-validation; values in brackets are 95% confidence intervals computed using the t-distribution.

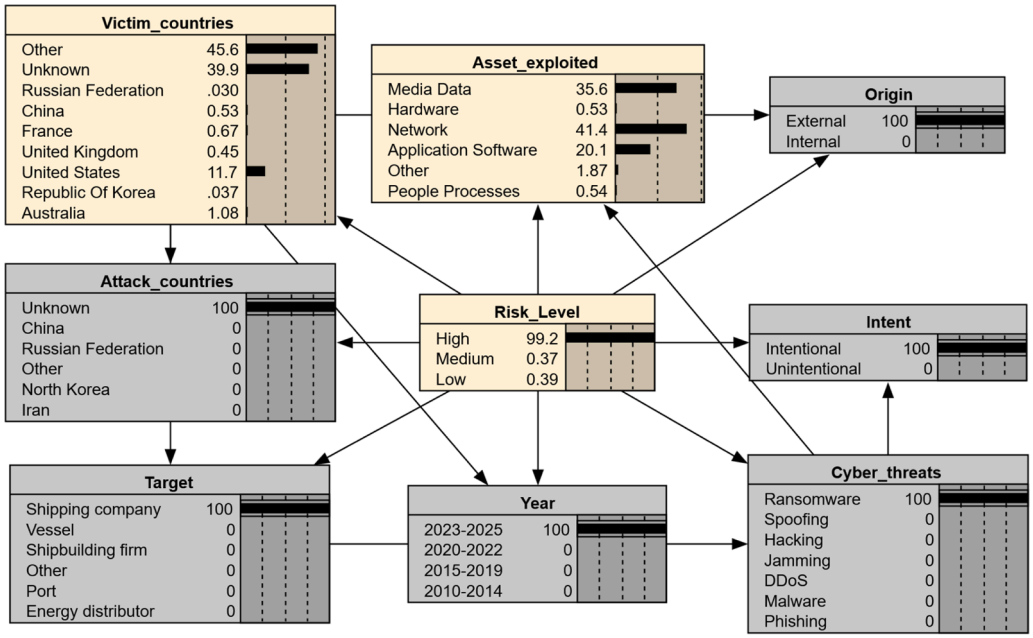


Fig. 9. Impact of attacker-related RIFs on high-risk levels.

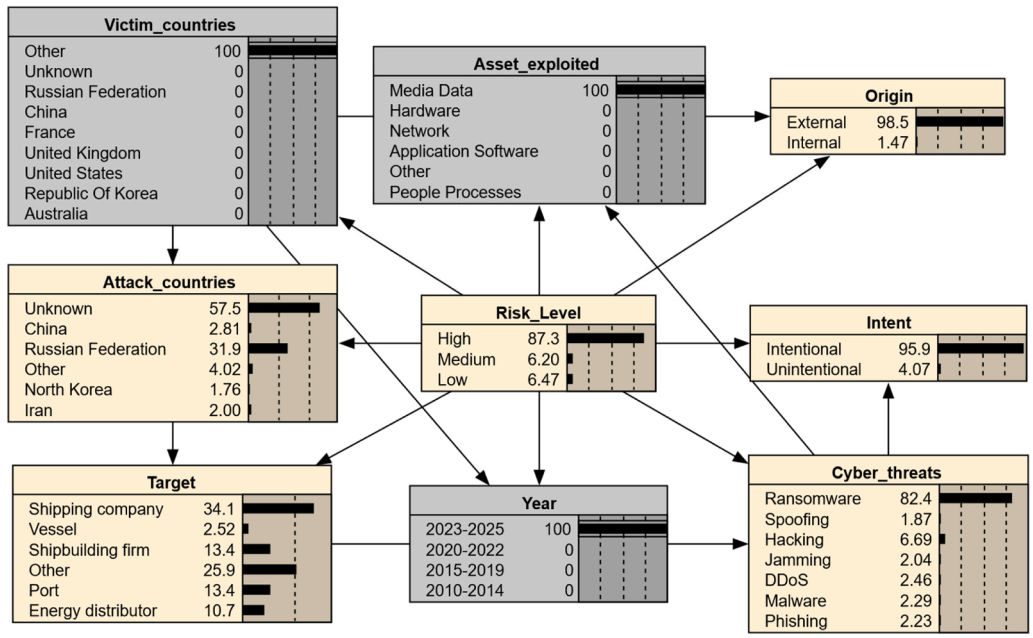


Fig. 10. The impact of RIFs related to victim countries on high-risk levels.

The scenario-level decomposition illustrates the distinction between incident frequency and relative risk contribution. Cluster 5, characterised primarily by ransomware-related business disruption, accounts for 47.5% of incidents but contributes 52.2% of the summed scenario-level risk scores. Its mean severity (0.657) exceeds the frequency-weighted sample mean (0.598), increasing its risk contribution relative to its incident share. By contrast, Clusters 2–4 have lower mean severity scores and consequently contribute smaller proportions of the summed relative risk than their respective incident shares. Cluster 1 has the second-highest mean severity but a lower incident frequency, resulting in a risk share of 15.9%. These differences indicate that frequency-based rankings may not fully reflect the relative importance of scenarios when consequence severity varies.

The spatial results provide a different perspective. The concentration of risk-weighted incidents in major maritime regions identifies locations where reported incidents with higher assigned scores are more prevalent. However, these concentrations cannot be attributed solely to differences in underlying cyber risk. Variations in maritime activity, digital infrastructure, incident disclosure and database coverage may all influence the observed patterns. The spatial analysis is therefore most informative for identifying areas that warrant further investigation, rather than establishing geographical differences in attack probability

The probabilistic analysis adds a further distinction between individual factor relevance and conditional dependence. Cyber Threats, Asset Exploited and Target provide the greatest information about the assigned risk levels, whereas Intent and Origin have comparatively low individual mutual information. The TAN model nevertheless allows relationships among predictors to be examined jointly. This is useful

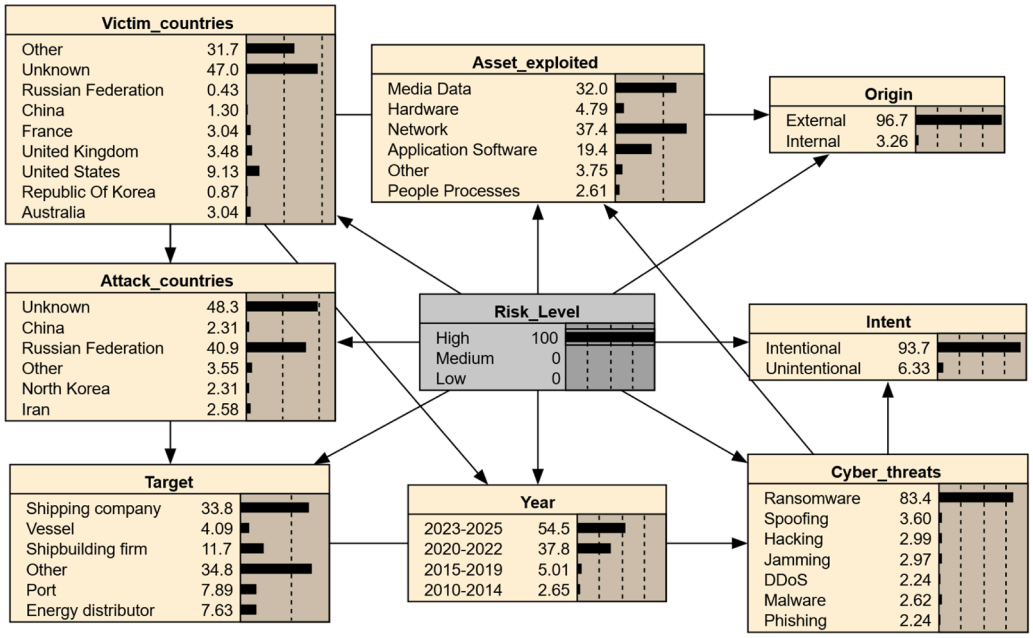


Fig. 11. Posterior probability distributions of the BN variables conditioned on a high risk level.

because a factor with limited individual discriminatory value may still contribute to classification when considered alongside other incident characteristics. The resulting network describes statistical dependencies in the MCAD records, not causal mechanisms linking attacker behaviour, system vulnerabilities and consequences

These findings support a layered interpretation of incident-based maritime cyber risk. Frequency–severity scoring identifies scenarios that merit closer examination; spatial analysis indicates where higher-scoring incidents are concentrated; and probabilistic modelling identifies characteristics associated with the assigned risk levels. The approaches provide different forms of evidence and should not be treated as interchangeable measures of risk. In particular, neither the spatial patterns nor the learned Bayesian network establishes how attacks propagate through interconnected maritime systems.

5.2. Limitations

Several limitations should be considered when interpreting the findings. First, the MCAD records are subject to incomplete coverage and reporting bias. Publicly disclosed and well-documented incidents are more likely to be included, while unreported or confidential events may be under-represented. Coverage also varies across years, regions and maritime sectors, and attacker attribution is incomplete for many incidents. These factors may influence the observed frequency and geographical distribution of reported incidents.

Second, the frequency–severity risk index provides relative comparisons within the MCAD sample rather than exposure-adjusted estimates of absolute risk. Consequence severity is represented by ordinal scores rather than calibrated measures of loss or operational disruption. Similarly, the spatial analysis identifies concentrations of reported incidents but does not account for differences in maritime activity, cyber exposure or reporting intensity. The resulting risk scores and hotspots should therefore be used for comparative assessment rather than as direct measures of attack probability or risk acceptability.

Third, the LCA and TAN models describe statistical patterns that depend on the available incident records and their classification. The TAN network represents conditional probabilistic associations rather than causal relationships, and its cross-validation performance has not been independently verified using external or prospective data. Furthermore, the dataset lacks detailed information on system vulnerabilities, operational dependencies and defensive controls, limiting the assessment of attack propagation and system-level consequences.

Future research should integrate additional incident sources with exposure, vulnerability and operational data, and evaluate model performance on independent datasets. These developments would help improve the robustness and practical applicability of maritime cyber-risk assessment.

5.3. Implications

The findings suggest several practical applications for maritime cyber-risk assessment, provided that the relative nature of the results is recognised.

For maritime operators, scenario-level risk comparisons can help identify attack types that warrant further assessment. The substantial contribution of ransomware-related business disruption suggests that continuity planning, recovery capability and the protection of business-critical digital services deserve particular attention. The distinction between incident frequency and severity also indicates that prioritisation should consider potentially disruptive but less frequent scenarios, rather than relying exclusively on historical incident counts.

For port authorities and maritime cybersecurity organisations, spatial concentrations can help guide more detailed investigations, information-sharing activities and the collection of supplementary evidence. Such patterns may inform where further assessment is needed, but they do not, by themselves, justify geographically differentiated regulatory requirements. Decisions of that kind require additional information on infrastructure criticality, exposure, vulnerability and existing safeguards.

The MI and TAN results may also inform the organisation of incident

reporting and threat analysis. The relatively high information content of threat type, exploited asset and target category supports the consistent recording of these attributes. Probabilistic dependencies can help analysts examine combinations of incident characteristics associated with different assigned risk levels. However, these relationships should be assessed against operational evidence before being used to guide specific defensive interventions.

More broadly, MC-QRA provides a structured basis for preliminary risk screening and comparative analysis using incident databases. Its outputs may complement established risk assessment practises, but they are not sufficient on their own to determine acceptable risk levels, quantify insurance exposure or optimise cybersecurity investment. Extending the approach to other critical infrastructure sectors would require suitable incident data, sector-specific consequence measures and validation of the resulting risk classifications.

6. Conclusions

This study developed MC-QRA, an integrated framework for assessing relative cyber risk in maritime systems using reported incident data. The framework combines LCA for scenario identification, frequency–severity risk scoring, KDE and Getis–Ord Gi* analysis for spatiotemporal assessment, and MI and TAN modelling for probabilistic dependency analysis. The empirical application used 444 incidents from the MCAD, following the exclusion of three pre-2010 records from a snapshot containing 447 incidents.

The analysis identified differences in scenario frequency, consequence severity, geographical concentration and the statistical associations between RIFs and assigned risk levels. Six main findings are summarised below.

(1) The number of reported maritime cyber incidents increased substantially over the study period, particularly after 2021. Medium- and high-risk incidents also became more prominent in the later years of the MCAD records. These trends describe changes in the reported sample and may partly reflect improvements in incident detection and reporting.
(2) Risk-weighted incident concentrations and statistically significant spatial clusters were identified in Europe, North America and East Asia. Their distribution also varied across the four study periods. These findings indicate geographical differences in the concentration of reported incidents, rather than exposure-adjusted differences in absolute cyber risk.
(3) Cyber Threats, Asset Exploited and Target were the most informative RIFs for distinguishing the assigned risk levels. The TAN results further identified conditional probabilistic dependencies among incident characteristics. These relationships should not be interpreted as causal effects or as verified evidence of attacker origin, particularly given the substantial proportion of records with incomplete geographical attribution.
(4) Business disruption was the most frequently recorded consequence type, followed by manipulation of maritime information and data breaches. Spoofing and jamming were prominent in scenarios involving vessel hardware and maritime information manipulation, whereas ransomware was closely associated with business disruption. These patterns illustrate the diversity of operational consequences represented in the MCAD records.
(5) Shipping companies and vessels featured prominently among the affected targets, while network and hardware assets were frequently recorded as exploited assets. These findings point to the importance of examining both organisational systems and operational technologies when assessing maritime cyber incidents.
(6) The frequency–severity decomposition showed that the ransomware-related scenario accounted for approximately 52.2% of the summed scenario-level relative risk scores, compared with 19.6% for the spoofing-related scenario. The difference between incident shares and risk shares demonstrates the importance of considering consequence severity alongside scenario frequency when prioritising incidents for further assessment.

The main contribution of MC-QRA lies in integrating established analytical methods into a common framework for scenario-level risk comparison, spatiotemporal analysis and probabilistic dependency assessment. The resulting risk scores are relative to the reported MCAD sample and are not estimates of absolute risk. Similarly, the spatial results are not normalised for exposure, and the TAN dependencies do not establish causality. The framework is therefore best used to support preliminary risk screening and prioritisation, rather than as a standalone basis for operational risk acceptance decisions.

Future research should incorporate operational exposure, system vulnerability and control-effectiveness data to support more detailed risk estimation. Multi-source intelligence could improve the attribution of incidents currently classified as Unknown or Others, while system topology and temporal evidence would be needed to investigate attack propagation. Further development of dynamic probabilistic models and the inclusion of organisational and human factors would also help extend the framework towards more comprehensive maritime cyber-risk assessment.

CRediT authorship contribution statement

Jincheng Gong: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Methodology, Investigation, Formal analysis, Data curation. **Yunfeng Zhao:** Writing – review & editing, Visualization, Validation, Software, Resources, Investigation, Formal analysis, Data curation. **Huanhuan Li:** Writing – review & editing, Writing – original draft, Visualization, Supervision, Software, Resources, Project administration, Methodology, Data curation, Conceptualization. **Zaili Yang:** Writing – review & editing, Visualization, Validation, Methodology, Funding acquisition, Formal analysis, Conceptualization.

Declaration of competing interest

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

Acknowledgements

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (Grant Agreement No. 864724).

Appendix A. Maritime cybersecurity keyword theme clustering

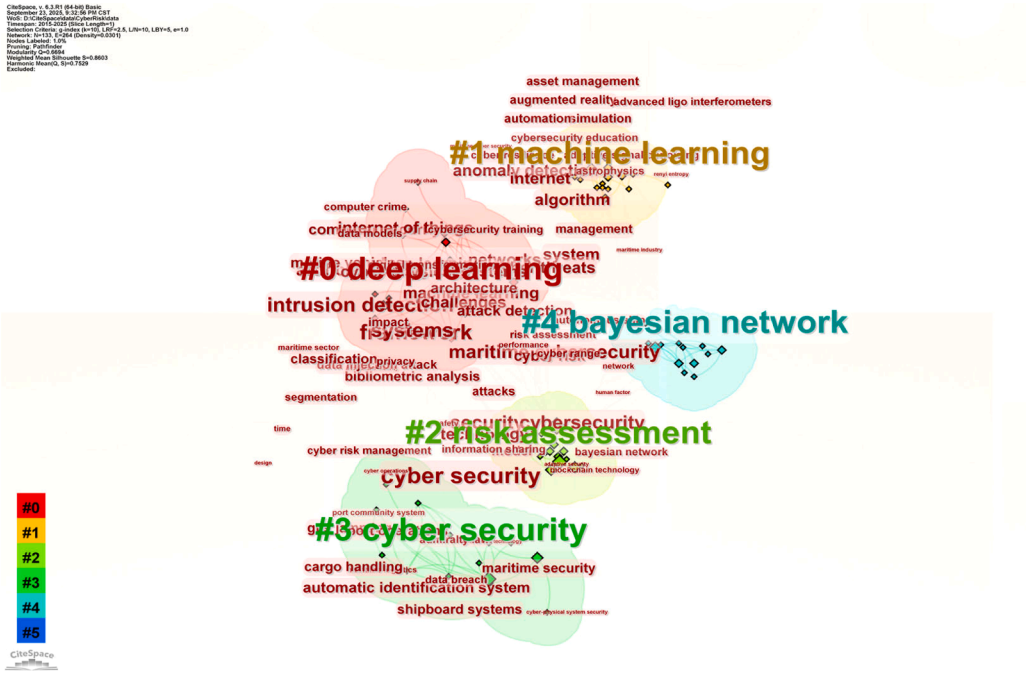


Fig. A.1. Keyword theme clustering diagram for maritime cybersecurity (2015–2025).

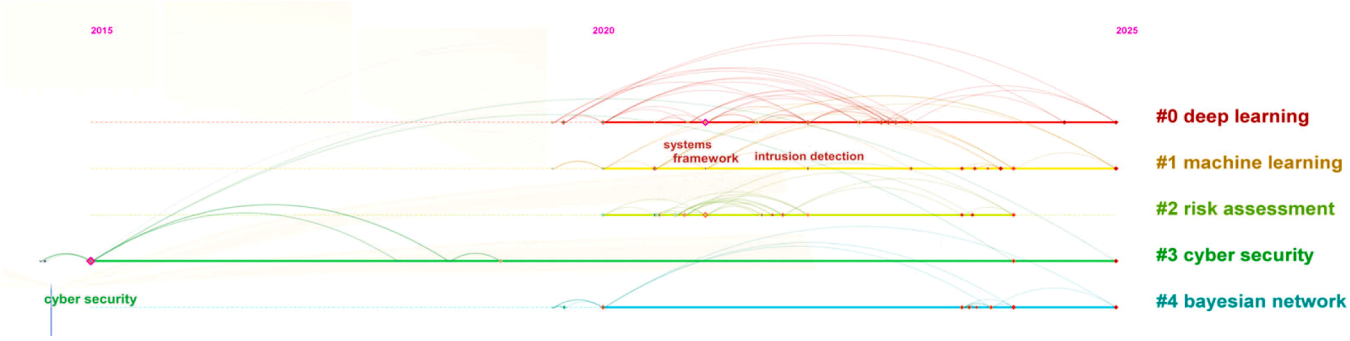


Fig. A.2. Maritime cybersecurity keyword timeline analysis (2015–2025).

Data availability

Data will be made available on request.

References

[1] Chen S, Meng B, Qiu B, Kuang H. Dynamic effects of maritime risk on macroeconomic and global maritime economic activity. Transp Policy 2025;167:246–63.

[2] Xu M, Ma X, Zhao Y, Qiao W. A systematic literature review of maritime transportation safety management. J Mar Sci Eng 2023;11:2311.

[3] Alavi A, Nguyen H-O, Fei J, Sayareh J. Port logistics integration: challenges and approaches. Int J Supply Chain Manag 2018;7:389–402.

[4] Gong J, Li H, Jiao H, Yang Z. Uncertainty-aware ship trajectory prediction via Spatio-Temporal graph transformer. Transp Res Part E Logist Transp Rev 2025;203:104315. https://doi.org/10.1016/j.tre.2025.104315.

[5] Kapidani N, Bauk S, Davidson IE. Digitalization in developing maritime business environments towards ensuring sustainability. Sustainability 2020;12:9235.

[6] Kaštelan N, Vidan P, Assani N, Miličević M. Digital horizon: assessing current status of digitalization in maritime industry. Trans Marit Sci 2024;13.

[7] Sanchez-Gonzalez P-L, Díaz-Gutiérrez D, Leo TJ, Núñez-Rivas LR. Toward digitalization of maritime transport? Sensors 2019;19:926.

[8] Mohsendokht M, Li H, Kontovas C, Chang C-H, Qu Z, Yang Z. Decoding dependencies among the risk factors influencing maritime cybersecurity: lessons learned from historical incidents in the past two decades. Ocean Eng 2024;312:119078. https://doi.org/10.1016/j.oceaneng.2024.119078.

[9] Maritime Cyber Attack Database (MCAD). Incident qZ3zEnboAK. 2025. https://maritimecybersecurity.nl/incident/qZ3zEnboAK. accessed October 15, 2025.

[10] Maritime Cyber Attack Database (MCAD). Incident 8dAmdRyoDM. 2025. https://maritimecybersecurity.nl/incident/8dAmdRyoDM. accessed October 15, 2025.

[11] Akpan F, Bendiab G, Shiaeles S, Karamperidis S, Michaloliakos M. Cybersecurity challenges in the maritime sector. Network 2022;2:123–38. https://doi.org/10.3390/network2010009.

[12] Afenyo M, Caesar LD. Maritime cybersecurity threats: gaps and directions for future research. Ocean Coast Manag 2023;236:106493.

[13] Kanwal K, Shi W, Kontovas C, Yang Z, Chang C-H. Maritime cybersecurity: are onboard systems ready? Marit Policy Manag 2024;51:484–502. https://doi.org/10.1080/03088839.2022.2124464.

[14] Pijpker J., McCombie S., Johnson S., Loves R., Makrakis G.M. An open-source database of cyberattacks on the maritime transportation system 2024.

[15] Zhao Y, Li H, Thanh Nguyen T, Matthews C, Yang Z. An automated bayesian network framework for maritime cybersecurity risk assessment powered by large language models. Saf Sci 2026;204:107384. https://doi.org/10.1016/j.ssci.2026.107384.

[16] Pranckutė R. Web of science (WoS) and Scopus: the titans of bibliographic information in Today's academic world. Publications 2021;9:12. https://doi.org/10.3390/publications9010012.

[17] Chen C, CiteSpace II. Detecting and visualizing emerging trends and transient patterns in scientific literature. J Am Soc Inf Sci Technol 2006;57:359–77. https://doi.org/10.1002/asi.20317.

[18] Ali Z, Hussain T, Su C-L, Jurcut AD, Baloch S, Sadiq M. Cyber attacks detection using deep learning methods for resilient operation in DC shipboard microgrids. IeeeIas Ind Commer Power Syst Asia Icps Asia 2024;2024:120–5. https://doi.org/10.1109/ICPSASIA61913.2024.10761631.
[19] Kumar P, Gupta GP, Tripathi R, Garg S, Hassan MM. DLTIF: deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled Maritime transportation systems. IEEE Trans Intell Transp Syst 2023;24:1–10. https://doi.org/10.1109/TITS.2021.3122368.
[20] Popli MS, Singh RP, Popli NK, Mamun M. A federated learning framework for enhanced data security and cyber intrusion detection in distributed network of underwater drones. Ieee Access 2025;13:12634–46. https://doi.org/10.1109/ACCESS.2025.3530499.
[21] Wilson A, Menzies R, Morarji N, Foster D, Mont MC, Turkbeyler E, et al. Multi-Agent reinforcement learning for maritime operational technology cyber security. 2024. Arxiv.
[22] Diaz R, Ungo R, Smith K, Haghnegahdar L, Singh B, Phuong T. Applications of AI /ML in maritime cyber supply chains. editors. In: Longo F, Shen W, Padovano A, editors. 5th Int. Conf. Ind. 40 Smart Manuf. Ism 2023232. Elsevier Science Bv; 2024. p. 3247–57. https://doi.org/10.1016/j.procs.2024.02.140.
[23] Aydin M, Sezer SI, Akyuz E, Gardoni P. Improved Z-number based bayesian network modelling to predict cyber-attack risk for maritime autonomous surface ship (MASS). Appl Soft Comput 2025;180:113416. https://doi.org/10.1016/j.asoc.2025.113416.
[24] Uflaz E, Sezer SI, Tuncel AL, Aydin M, Akyuz E, Arslan O. Quantifying potential cyber-attack risks in maritime transportation under Dempster-Shafer theory FMECA and rule-based Bayesian network modelling. Reliab Eng Syst Saf 2024;243:109825. https://doi.org/10.1016/j.ress.2023.109825.
[25] Haugli-Sandvik M, Lund MS, Bjorneseth FB. Maritime decision-makers and cyber security: deck officers' perception of cyber risks towards IT and OT systems. Int J Inf Secur 2024;23:1721–39. https://doi.org/10.1007/s10207-023-00810-y.
[26] Soner O, Kandemir C. Proposing the future skill requirements for maritime cyber security. Cogn Technol Work 2024;26:361–74. https://doi.org/10.1007/s10111-024-00760-y.
[27] Svilicic B, Kamahara J, Rooks M, Yano Y. Maritime Cyber risk Management: an experimental ship assessment. J Navig 2019;72:1108–20. https://doi.org/10.1017/S0373463318001157.
[28] Li J, Liu J, Wu Z, Wang J. FL-CGF: an edge-federated learning-based intelligent intrusion detection framework for heterogenous maritime internet of things. 2024 5th int. Conf Comput Big Data Artif Intell Iccbdai 2024:132–6. https://doi.org/10.1109/ICCBD-AI65562.2024.00030.
[29] Liu W, Xu X, Wu L, Qi L, Jolfaei A, Ding W, et al. Intrusion detection for maritime transportation systems with batch federated aggregation. IEEE Trans Intell Transp Syst 2023;24:1–12. https://doi.org/10.1109/TITS.2022.3181436.
[30] Bitit R., Guerroumi M., Derhab A. S2SCAF-BNRA: sequence to sequence based approach for cyber-attack forecasting with Bayesian network decision-making. 2024 1st Int Conf Electr Comput Telecommun Energy Technol Ecte-Tech, New York: IEEE; 2024, p. 13. https://doi.org/10.1109/ECTE-TECH62477.2024.10851070.
[31] Mahendran RK, Rajendran S, Pandian P, Rathore RS, Benedetto F, Jhaveri RH. A novel constructive unceasement conditional random field and dynamic bayesian network model for attack prediction on internet of vehicle. IEEE Access 2024;12:24644–58. https://doi.org/10.1109/ACCESS.2024.3363420.
[32] Tanwar M, Raghavan N, Dammala PK. Fault detection and isolation of cyber-physical system under cyber-attack using Bayesian network. In: 2024 IEEE Int. Conf. Progn. Health Manag. ICPHM 2024. IEEE; 2024. p. 84–92. https://doi.org/10.1109/ICPHM61352.2024.10627322.
[33] Zhang X, Zhang D. Quantitative risk assessment of Cyber physical power system using Bayesian based on Petri Net. In: Proc. 2018 5th Ieee Int. Conf. Cloud Comput. Intell. Syst. Ccis. IEEE; 2018. p. 988–92.
[34] Deng S, Zhang J, Wu D, He Y, Xie X, Wu X. A quantitative risk assessment model for distribution cyber-physical system under cyberattack. Ieee Trans Ind Inform 2023;19:2899–908. https://doi.org/10.1109/TII.2022.3169456.
[35] Le A, Chen Y, Chai KK, Vasenev A, Montoya L. Incorporating FAIR into Bayesian network for numerical assessment of loss event frequencies of smart grid cyber threats. Mob Netw Appl 2019;24:1713–21. https://doi.org/10.1007/s11036-018-1047-6.
[36] Gaskova DA, Massel AG. Semantic modeling of cyber threats in the energy sector using dynamic cognitive maps and Bayesian belief network. editors. In: Yusupova N, Shakhmametova G, Mironov K, Galimova L, editors. Proc. 7th Sci. Conf. Inf. Technol. Intell. Decis. Mak. Support Itids 2019. 166. Paris: Atlantis Press; 2019. p. 326–9.
[37] Park C, Kontovas C, Yang Z, Chang C-H. A BN driven FMEA approach to assess maritime cybersecurity risks. Ocean Coast Manag 2023;235:106480.
[38] Papageorgiou P, Dermatis Z, Anastasiou A, Liargovas P, Papadimitriou S. Using a proposed risk computation procedure and bow-tie diagram as a method for maritime security assessment. Transp Res Rec: J Transp Res Rec 2023;2678(2):318–39. https://doi.org/10.1177/03611981231173641. https://journals.sagepub.com/doi/10.1177/03611981231173641. [Accessed 30 June 2023].
[39] Progoulakis I, Dagkinis IK, Dimakopoulou A, Lilas T, Nikitakos N, Psomas PM. Cyber-physical security assessment for maritime vessels: study on drillship DP system using American Petroleum Institute Security risk analysis and bow-tie analysis. J Mar Sci Eng 2024;12:1757. https://doi.org/10.3390/jmse12101757.
[40] Bernsmed K, Froystad C, Meland PH, Nesheim DA, Rodseth OJ. Visualizing cyber security risks with bow-tie diagrams. editorsLiu P, Mauw S, Stolen K, editors. Visualizing cyber security risks with bow-tie diagrams. Graph Models Secur 2018;10744:38–56. https://doi.org/10.1007/978-3-319-74860-3_3.
[41] Fovino IN, Masera M, De Cian A. Integrating cyber attacks within fault trees. Reliab Eng Syst Saf 2009;94:1394–402. https://doi.org/10.1016/j.ress.2009.02.020.
[42] Nascimento L, de Oliveira AL, Villela R, Wei R, Hawkins R, Kelly T. From fault tree analysis to runtime model-based assurance cases. editorBarolli L, editor. From fault tree analysis to runtime model-based assurance cases. Adv Inf Netw Appl 2024;200:451–64. https://doi.org/10.1007/978-3-031-57853-3_38. Vol 2 Aina 2024.
[43] Niloofar P, Lazarova-Molnar S. Fusion of data and expert knowledge for fault tree reliability analysis of cyber-physical systems. In: 2021 5th Int. Conf. Syst. Reliab. Saf. Icsrs 2021. IEEE; 2021. p. 92–7. https://doi.org/10.1109/ICSRS53853.2021.9660717.
[44] Kumar R, Stoelinga M. Quantitative security and safety analysis with attack-fault trees. In: 2017 Ieee 18th Int. Symp. High Assur. Syst. Eng. Hase 2017. IEEE; 2017. p. 25–32. https://doi.org/10.1109/HASE.2017.12.
[45] Weglian JE, Riley J, Gibson M. Integrating fault tree analysis with system theoretic process analysis. In: 2023 Annu. Reliab. Maintainab. Symp. Rams. IEEE; 2023. https://doi.org/10.1109/RAMS51473.2023.10088187.
[46] Zhang F, Yang J, Li J, Zhang J, Li J, Chen L, et al. Integrated physical safety-cyber security risk assessment based on layers of protection analysis. Chem Eng Res Des 2024;212:405–20. https://doi.org/10.1016/j.cherd.2024.10.036.
[47] Son K-S, Song J-G, Lee J-W. Development of the framework for quantitative cyber risk assessment in nuclear facilities. Nucl Eng Technol 2023;55:2034–46. https://doi.org/10.1016/j.net.2023.03.023.
[48] Zhou Y, Zhang Z, Fan K, Wang M, Cheng K, Zhang Z, et al. A novel quantitative risk assessment model for industrial control systems integrating the cyber-physical domain. IEEE Trans Ind Inform 2025;21:6433–42. https://doi.org/10.1109/TII.2025.3564074.
[49] Alguliyev R, Aliguliyev R, Sukhostat L. Method for quantitative risk assessment of cyber-physical systems based on vulnerability analysis. Kybernetika 2024;60:779–96. https://doi.org/10.14736/kyb-2024-6-0779.
[50] Mohsendokht M, Li H, Kontovas C, Chang C, Qu Z, Yang Z. Enhancing maritime transportation security: a data-driven Bayesian network analysis of terrorist attack risks. Risk Anal 2025;45:283–306. https://doi.org/10.1111/risa.15750.
[51] Zhao Y, Li H, Nguyen TT, Matthews C, Yang Z. Integrating prompt-based zero-shot learning into Bayesian network for maritime cybersecurity risk analysis. Transp Res Part E: Logist Transp Rev 2026;216:105134. https://doi.org/10.1016/j.tre.2026.105134. https://linkinghub.elsevier.com/retrieve/pii/S1366554526004722. 105134.
[52] Zhao Y, Gong J, Li H, Nguyen TT, Matthews C, Yang Z. Cybersecurity in smart port systems: A systematic review and data-driven research agenda. Transp Policy 2026;187:104268. https://doi.org/10.1016/j.tranpol.2026.104268. https://linkinghub.elsevier.com/retrieve/pii/S0967070X26002787. 104268.
[53] Ren Q, Xu M. Heterogeneity in crash patterns of autonomous vehicles: the latent class analysis coupled with multinomial logit model. Accid Anal Prev 2025;209:107827. https://doi.org/10.1016/j.aap.2024.107827.
[54] Liang M, Li H, Liu RW, Lam JSL, Yang Z. PiracyAnalyzer: Spatial temporal patterns analysis of global piracy incidents. Reliab Eng Syst Saf 2024;243:109877.
[55] Chen Y-C. A tutorial on kernel density estimation and recent advances. Biostat Epidemiol 2017;1:161–87. https://doi.org/10.1080/24709360.2017.1396742.
[56] Rong H, Teixeira AP, Guedes Soares C. Spatial correlation analysis of near ship collision hotspots with local maritime traffic characteristics. Reliab Eng Syst Saf 2021;209:107463. https://doi.org/10.1016/j.ress.2021.107463. https://linkinghub.elsevier.com/retrieve/pii/S0951832021000314. 107463.
[57] Dinh T, Wong H, Fournier-Viger P, Lisik D, Ha M-Q, Dam H-C, et al. Categorical data clustering: 25 years beyond K-modes. Expert Syst Appl 2025;272:126608. https://doi.org/10.1016/j.eswa.2025.126608.
[58] Kordestani M, Rezamand M, Orchard ME, Saif M. Condition-based maintenance scheduling using probability distribution function and agglomerative hierarchical clustering approaches: al-driven predictive maintenance mapping. IEEE Syst Man Cybern Mag 2025;11:61–72. https://doi.org/10.1109/MSMC.2024.3509826.
[59] Guha S, Rastogi R, Shim K. Rock: a robust clustering algorithm for categorical attributes. Inf Syst 2000;25:345–66. https://doi.org/10.1016/S0306-4379(00)00022-3.
[60] Li H, Jiao H, Chen ZS, Lam JSL, Yang Z. COVID crisis-aware maritime risk assessment: a bayesian network analysis. Reliab Eng Syst Saf 2025:111783.
[61] Wu Y, Li H, Jiao H, Chen ZS, Murphy AJ, Yang Z. Impact of voyage segments on maritime accidents: an analysis of navigational factors and accident causes. Reliab Eng Syst Saf 2026;270:112188.