Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
©2025 ESREL SRA-E 2025 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P0401-cd

A New AI Solution to Maritime Cybersecurity Risk Prediction

Yunfeng Zhao

Liverpool Logistics, Offshore and Marine (LOOM) Research Institute, Liverpool John Moores University, United Kingdom. E-mail: y.zhao1@2024.ljmu.ac.uk

Huanhuan Li

Liverpool Logistics, Offshore and Marine (LOOM) Research Institute, Liverpool John Moores University, United Kingdom. E-mail: h.li2@ljmu.ac.uk

Zaili Yang

Liverpool Logistics, Offshore and Marine (LOOM) Research Institute, Liverpool John Moores University, United Kingdom. E-mail: z.yang@ljmu.ac.uk

Abstract: The digitalisation of maritime systems, including ships, ports, and operational networks, has significantly increased their exposure to cyber threats and risks. These risks can disrupt critical infrastructure and cause global repercussions, requiring new solutions to improve maritime cybersecurity risk prediction. This study aims to develop a new AI solution with limited data to enable cybersecurity risk prediction. It utilises Large Language Models (LLMs) for prompt-based zero-shot learning, enabling accurate classification of text and extraction of key cyber risk factors. A comprehensive dataset spanning 2001 to 2020 was developed, introducing new risk factors critical for assessing cyber threats that are yet to appear in any state-of-the-art studies in the field. This extracted dataset was integrated into a Bayesian Network (BN) model to identify probabilistic relationships and predict potential cybersecurity risks. The hybrid approach is among the pioneers of using new AI technologies for text mining to enrich risk data and realising multiple source data fusion for improved risk prediction, hence making significant theoretical contributions to safety sciences. By leveraging the advanced capabilities of LLMs alongside probabilistic modelling, the study has shown its methodological novelty through a scalable, adaptive methodology that can enhance risk predictive accuracy and strengthen general and maritime systems against evolving cyber risks in specific. From an applied research perspective, it provides an in-depth analysis of maritime cybersecurity within the context of the fast growth of maritime digitalisation and brings significant managerial insights into practice. Such insights are invaluable for stakeholders, enabling them to identify vulnerabilities, anticipate threats, and prioritise resources effectively. This integrated framework equips policymakers with the tools needed for proactive decision-making, supporting the development of targeted cybersecurity strategies to minimise operational disruptions.

Keywords: Maritime Cybersecurity, Large Language Models, Zero-shot Learning, Bayesian Network, Risk Analysis

1. Introduction

Maritime transport is important in global trade, facilitating the movement of goods and resources across continents and supporting economic stability worldwide (Li and Yang, 2023). With over 80% of international trade dependent on maritime transport, the industry plays a crucial role in connecting global markets, particularly in regions characterised by extensive waterways and coastal economies (Cao et al., 2023; Li et al., 2024a). As international trade expands due to globalisation, population growth, and rising living standards, the maritime sector has embraced technological advancements to enhance efficiency, sustainability, and environmental friendliness. Emerging technologies such as the Internet of Things (IoT), big data analytics, and Artificial Intelligence (AI) have enabled the transition from traditional maritime operations to interconnected and digitalised infrastructures (Bures et al., 2021).

However, this digital transformation has introduced significant cybersecurity challenges. The increasing reliance on interconnected systems has amplified vulnerabilities, making maritime infrastructures—such as vessels, ports, and operational networks—prime targets for cyberattacks (de la Peña Zarzuelo, 2021). Cyber threats range from phishing and ransomware to advanced methods that exploit weak points in navigation systems, communication networks, and operational frameworks. The implications of such attacks extend far beyond financial losses, affecting global supply chains, economic stability, and environmental safety. This growing risk highlights the urgent need for a comprehensive and adaptive maritime cybersecurity framework to protect critical assets and ensure operational resilience.

Traditional approaches to maritime cybersecurity risk analysis often rely on qualitative methods, such as expert-driven insights and risk matrices, which are prone to subjective biases and limited scalability. While quantitative risk analysis methods, including the Bayesian Network (BN) (Li et al., 2024b; Mohsendokht et al., 2025), offer a more objective approach by modelling probabilistic relationships between risk factors, they require extensive and well-structured datasets to deliver accurate results. This results in their inability to tackle maritime cybersecurity risk quantification and prediction. In the maritime sector, the scarcity of high-quality, labelled datasets poses a significant challenge for implementing robust cybersecurity models. This limitation is further compounded by the evolving nature of cyber threats, which necessitates new cyber risk analysis frameworks by AI powers in text mining and data training.

To address these challenges, this study proposes an innovative hybrid approach that integrates prompt-based zero-shot learning with BN modelling. The application of Large Language Models (LLMs) within this framework allows for the extraction of nuanced risk factors from unstructured textual data, such as cybersecurity incident reports, even in the absence of labelled datasets. Prompt-based zero-shot learning leverages pre-trained LLMs to classify and extract critical information with minimal training data (Brown et al., 2020), making it an efficient solution for data-scarce environments like maritime cybersecurity. The extracted risk factors are then incorporated into a BN framework, enabling the modelling of probabilistic relationships, identification of interdependencies, and prediction of potential cyberattack scenarios.

By leveraging advanced AI-driven methodologies and addressing critical gaps in traditional risk analysis approaches, this research aims to develop a scalable and adaptive framework for maritime cybersecurity risk prediction. This novel approach not only improves predictive accuracy but also empowers decision-makers with the tools needed to navigate the complexities of an increasingly digitalised and interconnected maritime domain. As the sector continues to evolve, this study lays the foundation for a more secure and resilient future in global maritime operations.

This study proceeds as follows: Section 2 explores the existing body of literature, emphasising key advancements and unresolved challenges in maritime cybersecurity. Section 3 details the methodological framework employed in this research, including the integration of advanced analytical techniques. Section 4 focuses on validating the proposed model and discussing the results in depth. Lastly, Section 5 concludes the study.

2. Literature review

Over the past decade, numerous studies have focused on developing robust frameworks and methodologies to identify, assess, and mitigate cybersecurity risks within the maritime sector. A notable contribution is the Maritime Cyber Risk Assessment (MaCRA) framework by Tam and Jones (2019), which provides a model-based approach to identifying critical risks, potential attackers, attack vectors, and systems requiring enhanced security. Similarly, Söner et al. (2023) utilised a Failure Mode and Effects Analysis (FMEA)-based approach to assessing cybersecurity risks associated with the Voyage Data Recorder (VDR), highlighting specific vulnerabilities in this critical component. Hybrid methods have also gained traction, such as the integration of FMEA with BN by Park et al. (2023), enabling a structured and quantitative evaluation of cyber-attack risks. However, most of these studies are qualitative analyses and rely on subjective data primarily collected through expert judgment. Since expert opinions inherently involve biases, this approach is prone to controversy. The reliability of the research depends on factors such as the number of experts responding to the questionnaire and the quality of their responses.

To address the complexity of cybersecurity challenges, researchers have increasingly turned to quantitative and hybrid approaches that combine traditional risk assessment with advanced probabilistic models. BN have proven particularly effective in this context due to their ability to represent dependencies among risk factors and predict potential outcomes. Previous studies in the relevant literature (e.g. Mohsendokht et al. 2024) demonstrate the efficacy of BN in maritime risk analysis, leveraging historical data to quantify the likelihood and consequences of cyber-attacks. The shift toward integrated methodologies reflects the growing recognition of the multidimensional nature of maritime cybersecurity risks, which require a combination of machine learning, probabilistic modelling, and scenario simulations to capture their full scope. Nevertheless, due to the typically limited size of maritime cyber attack datasets, the manually extracted Risk Influential Factors (RIFs) do not fully cover all cyberattack scenarios. It is crucial to leverage advanced AI methods to overcome this limitation, particularly in data processing, as this plays a vital role in subsequent research and analysis.

Traditional text classification methods in NLP, such as rule-based approaches and Machine Learning (ML) models, rely heavily on feature engineering to classify and interpret textual data. While effective for structured tasks, these methods struggle to capture the complexity and nuances of natural language, especially in unstructured datasets (Keerthi et al., 2001; Xu et al., 2012). In contrast, Deep Learning (DL) models, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), enhance performance by automating feature extraction. However, they require large labelled datasets and substantial computational resources. The advent of LLMs, such as Bidirectional Encoder Representations from Transformers (BERT) (Devlin, 2018), Text-to-Text Transfer Transformer (T5) (Raffel et al., 2023), Generative Pre-trained Transformer 3 (GPT-3) (Brown et al., 2020), and Large Language Model Meta AI (LlaMA) (Touvron et al., 2023), has revolutionised text classification by enabling zero-shot and few-shot learning capabilities. Although showing attractiveness, these models that can leverage pre-trained knowledge to perform specific tasks with minimal labelled data have yet to be applied to predict maritime cybersecurity risks. To make them effective in the data-scarce context of maritime cybersecurity, prompt-based zero-shot learning is applied in this work, allowing LLMs to extract nuanced risk factors from textual data without extensive preprocessing, providing a powerful tool for analysing maritime cybersecurity reports. This approach has demonstrated remarkable efficiency in identifying previously underexplored or complex risk factors, contributing to a deeper understanding of the threats facing the maritime sector.

The new framework proposed in this paper will bridge the mentioned gaps, offering improved predictive accuracy and scalability. By focusing on evolving cyber threats, the methodology provides a dynamic and responsive tool for mitigating risks and enhancing maritime system resilience. As cyberattacks grow more sophisticated, this integrated approach supports proactive strategies to safeguard critical infrastructure and operations globally.

3. Methodology

3.1. *Dataset generation*

To support advancements in maritime cybersecurity research, the creation of a comprehensive and reliable dataset is essential. This study utilised a systematic process to compile and refine a dataset specifically focused on maritime cyber-attacks. The Maritime Cyber Attack Database (MCAD), an open-source resource curated by the Maritime IT Security Research Group at NHL Stenden University of Applied Sciences in the Netherlands, served as the primary data source (MCAD, 2024). In this study, a total of 138 maritime-specific cyber incident records from the MCAD dataset spanning 2001 to 2020 were extracted for testing, providing a valuable foundation for further research and analysis. The following methodology is applied to collect, cleanse, and structure the data into a usable format.

The data collection process employed an automated web crawler to extract information from publicly available maritime cybersecurity sources. This crawler gathered incident details such as the date, attacker and victim countries, attack methods, impacted areas, and incident reports. The open-source nature of the web crawler ensures transparency and encourages replicability for future studies, allowing researchers to build upon this initial dataset. The collected data offers a wealth of insights into the characteristics and consequences of cyber-attacks within the maritime sector.

Following data collection, a rigorous data cleansing was undertaken to ensure quality and accuracy. Duplicate records were removed to eliminate redundancies, while incomplete or invalid entries—such as those lacking critical fields or containing empty summaries—were excluded. Non-visible characters, which could interfere with text analysis by LLMs, were also identified and removed. This multi-step cleansing process ensured that the dataset retained only valid and relevant information, providing a solid basis for further processing and analysis.

By implementing these steps, a robust and reliable dataset was created, forming the foundation for the application of advanced methodologies such as prompt-based zero-shot learning and BN modelling in maritime cybersecurity research. This dataset not only supports the objectives of the current study but also serves as a critical resource for future explorations in the field.

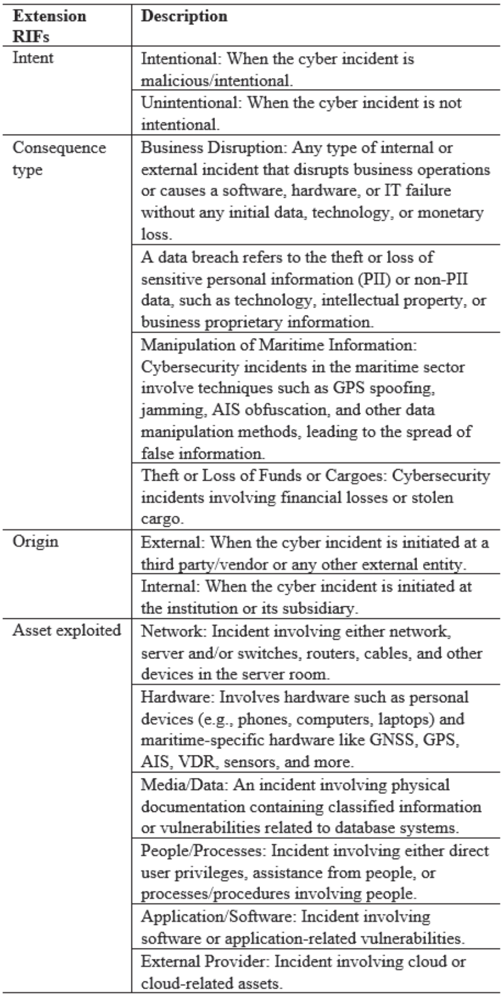
3.2. *Definifation and identification of RIFs*

A comprehensive understanding of cyber risks in the maritime domain relies on the precise identification and definition of RIFs. These factors serve as the foundation for effective data analysis, classification, and modelling in cybersecurity studies. This research undertook a rigorous process to define and expand the scope of RIFs, ensuring a more detailed and structured framework for analysing maritime cybersecurity risks.

The original RIFs from the MCAD dataset include “Year”, “Attacker country”, “Victim country”, “method”, and “Impact area”. For detailed descriptions of these RIFs, please refer to the referenced sources (MCAD, 2024; Mohsendokht et al., 2024). Drawing from a thorough literature review of cybersecurity of the other sectors, four new RIFs were developed and incorporated into this study: “Intent”, “Origin”, “Asset Exploited”, and “Consequence Type”. These factors were specifically designed to enrich the analysis by capturing motivations, vulnerabilities, and impacts more comprehensively. The overview of four extended RIFs is listed in Table 1.

Clearly defining and generating RIFs significantly enhances the granularity of maritime cybersecurity analysis. By integrating factors related to motivations, origins, vulnerabilities, and consequences, this study provides a comprehensive framework for understanding maritime cyber risks.

Table 1. The overview of four extended RIFs.



Extension RIFs	Description
Intent	Intentional: When the cyber incident is malicious/intentional.
	Unintentional: When the cyber incident is not intentional.
Consequence type	Business Disruption: Any type of internal or external incident that disrupts business operations or causes a software, hardware, or IT failure without any initial data, technology, or monetary loss.
	A data breach refers to the theft or loss of sensitive personal information (PII) or non-PII data, such as technology, intellectual property, or business proprietary information.
	Manipulation of Maritime Information: Cybersecurity incidents in the maritime sector involve techniques such as GPS spoofing, jamming, AIS obfuscation, and other data manipulation methods, leading to the spread of false information.
	Theft or Loss of Funds or Cargoes: Cybersecurity incidents involving financial losses or stolen cargo.
Origin	External: When the cyber incident is initiated at a third party/vendor or any other external entity.
	Internal: When the cyber incident is initiated at the institution or its subsidiary.
Asset exploited	Network: Incident involving either network, server and/or switches, routers, cables, and other devices in the server room.
	Hardware: Involves hardware such as personal devices (e.g., phones, computers, laptops) and maritime-specific hardware like GNSS, GPS, AIS, VDR, sensors, and more.
	Media/Data: An incident involving physical documentation containing classified information or vulnerabilities related to database systems.
	People/Processes: Incident involving either direct user privileges, assistance from people, or processes/procedures involving people.
	Application/Software: Incident involving software or application-related vulnerabilities.
	External Provider: Incident involving cloud or cloud-related assets.

3.3. *Prompt engineering-based BN modelling*

With a clear definition of RIFs, this study proposes an automated text classification method, which can significantly reduce biases associated with manual or expert classification and improve classification accuracy. By using AI-driven tools, the framework classifies textual data with precision that reflects the intricate relationships influencing cybersecurity risks within the maritime domain.

Prompt engineering enables accurate classification of RIFs from unstructured cyber-attack reports by using carefully crafted textual prompts. Traditional classification methods face challenges in scenarios with limited labelled data, as is common in maritime cybersecurity. By adopting a zero-shot prompting strategy, this study overcomes these limitations, allowing for high-quality classification without requiring extensive training data. LLMs like GPT-4 (Mao et al., 2024), which possess pre-trained knowledge across a vast corpus of text, are used to classify critical risk factors such as "Consequence Type," "Asset Exploited," "Intent," and "Origin," based on the refined dataset. These well-defined RIFs enrich the analysis, capturing essential attributes and offering deeper insights into maritime cybersecurity threats.

The prompt engineering process was carefully tailored to ensure accuracy and interpretability. To enhance programmatic accessibility, output responses were formatted in JavaScript Object Notation (JSON), while reasoning requirements aligned with the Chain of Thought (CoT) prompting principles (Wei et al., 2022). This approach not only improved transparency but also enhanced the accuracy of classifications by requiring the model to explain its decisions systematically. For instance, when categorising "Consequence Type," the prompt explicitly instructed the model to identify the impact type while justifying its classification. This iterative design enabled continuous refinement and debugging, further improving the classification performance.

Following the prompt-based classification, the enriched dataset was integrated into a BN framework to model the probabilistic relationships among the identified RIFs. In this step, a Tree Augmented Naïve (TAN)-based data-driven BN model is applied. Specifically, TAN used "Consequence Type" as the target node, reflecting its significance in understanding the broader implications of cyber incidents.

The BN was constructed using the classified data and developed using Netica software. The TAN structure visualised in this model reveals the interconnected dynamics of maritime cybersecurity risks. For example, it illustrates how an external origin attack targeting critical hardware might lead to specific consequence types, such as business disruptions or data breaches. This structured representation enhances interpretability, making the model a powerful tool for scenario-based risk assessments and real-time decision-making. The constructed BN model is presented in Fig. 1.

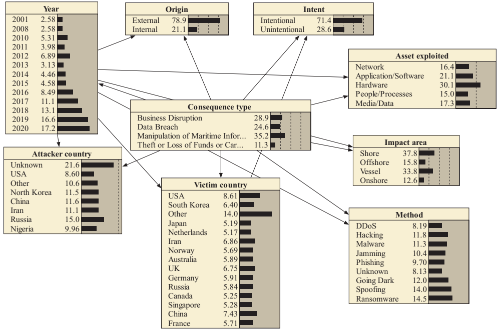


Fig. 1. The prompt engineering-based BN modelling.

4. Model validation and analysis

4.1. *Mutual information*

Mutual Information (MI) (Wu et al., 2020) quantifies the dependency between the target node, "Consequence Type," and other variables in the BN, reflecting how much knowledge of one variable reduces uncertainty about another. In this study, MI was calculated to evaluate the influence of different factors on "Consequence Type," with the results presented in Table 2. These values highlight the degree of dependence between the target node and its associated factors, providing insight into their relevance for maritime cybersecurity risk modelling.

The "Consequence Type" node had the highest MI value, underscoring its central role in the BN for predicting cybersecurity risks. Among other variables, "Asset Exploited" had the strongest dependency (0. 25634), emphasising the critical role of the targeted asset, such as hardware or software, in determining the consequences of cyberattacks. Temporal patterns, represented by the "Year" variable (0.21201), also played a significant role, indicating that evolving attack techniques and changes in cybersecurity practices over time notably impact outcomes.

Moderate dependencies were observed for "Impact Area" (0.17675) and "Method" (0.139), showing the importance of attack locations and techniques in shaping cyber incident consequences. Factors like "Attacker Country," "Victim Country," "Origin," and "Intent" exhibited lower MI values, indicating weaker but still relevant relationships with "Consequence Type." These insights help prioritise high-impact factors, allowing stakeholders to focus on protecting critical assets and addressing emerging attack methods. The analysis demonstrates how the BN model provides actionable insights to enhance decision-making and build resilient maritime cybersecurity systems.

Table 2. The results of MI.

Node	MI
Consequence type	1.90061
Asset exploited	0.25634
Year	0.21201
Impact area	0.17675
Method	0.13900
Attacker country	0.06303
Victim country	0.03145
Intent	0.00351
Origin	0.00337

4.2. *True risk influence*

The True Risk Influence (TRI) (Alyami et al., 2019) metric quantifies the impact of each RIF on the target node, "Consequence Type," across various outcomes such as Business Disruption, Data Breach, Manipulation of Maritime Information, and Theft or Loss of Funds or Cargoes. Table 3 presents the TRI values for each RIF, highlighting their relative importance in predicting specific consequences.

"Asset Exploited" emerges as the most influential factor, with an average TRI of 19.9, particularly for Manipulation of Maritime Information (28.1), emphasising the importance of safeguarding critical assets like hardware and software. Similarly, "Year" (average TRI: 19.6) ranks as a key determinant, reflecting the critical role of temporal trends in shaping cyber incidents. It has the highest TRI for Business Disruption (20.2) and Manipulation of Maritime Information (23.2), underscoring the impact of evolving attack techniques and technologies over time.

Other factors such as "Impact Area" (average TRI: 17.3) and "Method" (15.7) show moderate influence, highlighting the significance of attack locations and techniques. Meanwhile, "Origin" (1.6) and "Intent" (1.2) exhibit lower TRI values, offering context but less direct impact on outcomes. These findings help prioritise high-impact factors, enabling stakeholders to allocate resources effectively and enhance maritime cybersecurity resilience.

Table 3. TRI of RIFs for the target node.

	S1	S2	S3	S4	Average
Asset exploited	18.3	19.9	28.1	13.5	19.9
Year	20.2	18.2	23.2	16.9	19.6
Impact area	22.3	18.6	27.5	0.9	17.3
Method	15.6	10.6	24.2	12.4	15.7
Attacker country	12.9	4.9	11.9	12.8	10.6
Victim country	7	7.2	10.2	3.1	6.9
Intent	0	0.45	1.9	2.4	1.2
Origin	0.7	0.3	3.1	2.3	1.6

Note: S1 indicates Business Disruption, S2 means Data Breach, S3 is Manipulation of Maritime Information, and S4 represents Theft or Loss of Funds or Cargoes.

4.3. *Model prediction performance*

The BN model's performance was assessed using a confusion matrix to evaluate its accuracy in predicting "Consequence Type" across four categories: Business Disruption, Data Breach, Manipulation of Maritime Information, and Theft or Loss of Funds or Cargoes. Table 4 summarises the results, including correctly classified instances, misclassifications, and accuracy rates.

The model achieved an accuracy of 96.9% for Business Disruption, correctly classifying 31 out of 32 instances and 94.1% for Data Breach, with 16 out of 17 instances correctly identified. For Manipulation of Maritime Information and Theft or Loss of Funds or Cargoes, the model reached a perfect accuracy of 100%, successfully classifying all instances.

Overall, the model correctly classified 62 out of 64 instances, yielding an accuracy rate of 96.9%. These results highlight the model's reliability in leveraging probabilistic relationships between RIFs and "Consequence Type." The high accuracy across all categories underscores its effectiveness in supporting decision-making and prioritising risk mitigation strategies for maritime cybersecurity.

Table 4. Confusion matrix of predicted results.

Actual Predicted	S1	S2	S3	S4	Actual total	Accuracy rate (%)

S1	7	0	0	1	8	87.5
S2	0	6	0	0	6	100
S3	0	0	9	0	9	100
S4	0	0	0	3	3	100
Total	7	6	9	4	26	96.2

4.4. *Model consistency verification*

Ensuring the reliability of a predictive model is critical for its effective application in real-world scenarios. To evaluate the consistency of the proposed model in predicting maritime collision accidents, Cohen's Kappa statistic (k) was utilised. This statistical measure assesses the agreement between predicted and actual classifications while accounting for the possibility of random agreement. A Kappa value closer to 1 indicates a higher degree of consistency and reliability in the model's performance (Fleiss, 1971; Li et al., 2023).

In this study, the model achieved a Kappa coefficient of k=0.945, indicating a very high level of agreement. This result confirms the model's excellent consistency and reliability in classifying collision risks under various conditions.

5. Conclusion

This study addresses the growing cybersecurity challenges posed by the digitalisation of maritime systems by introducing an innovative framework that combines LLMs with BN modelling. By leveraging prompt-based zero-shot learning, the framework effectively classifies text and extracts key cyber risk factors from limited datasets, enabling comprehensive risk analysis. The developed dataset, spanning from 2001 to 2020, incorporates four novel risk factors to enhance the granularity of maritime cybersecurity risk assessment. The integration of this enriched dataset into a BN model allows for the identification of probabilistic relationships and an in-depth evaluation of how various factors influence the likelihood and severity of cybersecurity incidents. This approach provides a nuanced understanding of maritime cybersecurity risks, equipping stakeholders with actionable insights to address vulnerabilities and enhance system resilience.

The hybrid methodology offers a scalable and adaptive approach to maritime cybersecurity risk management, enhancing predictive accuracy and supporting proactive decision-making. By mapping interdependencies among risk factors, this study highlights the value of advanced technologies like LLMs and probabilistic modelling in addressing emerging threats. The proposed framework strengthens cybersecurity strategies, minimises disruptions, and enhances global maritime security.

Future research can further leverage LLMs for analysing unstructured text. Techniques, like Named Entity Recognition (NER), can extract key entities, while Topic Modeling (TM) can identify hidden risk patterns. These approaches will refine maritime cybersecurity analysis, providing deeper insights and improving risk mitigation strategies.

Acknowledgement

This research was funded by a European Research Council project under the European Union's Horizon 2020 research and innovation programme (TRUST CoG 2019 864724).

References

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

Brown, T.B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D.M., Wu, J., Winter, C., Hesse, C., Chen, M., Sigler, E., Litwin, M., Gray, S., Chess, B., Clark, J., Berner, C., McCandlish, S., Radford, A., Sutskever, I., Amodei, D., 2020. Language Models are Few-Shot Learners.

Bures, M., Ahmed, B.S., Rechtberger, V., Klima, M., Trnka, M., Jaros, M., Bellekens, X., Almog, D., Herout, P., 2021. Patriot: Iot automated interoperability and integration testing framework, in: 2021 14th IEEE Conference on Software Testing, Verification and Validation (ICST). IEEE, pp. 454–459.

Cao, Y., Wang, X., Yang, Z., Wang, J., Wang, H., Liu, Z., 2023. Research in marine accidents: A bibliometric analysis, systematic review and future directions. Ocean Engineering 284, 115048. https://doi.org/10.1016/j.oceaneng.2023.115048

de la Peña Zarzuelo, I., 2021. Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. Transport Policy 100, 1–4.

Devlin, J., 2018. Bert: Pre-training of deep bidirectional transformers for language understanding. arXiv preprint arXiv:1810.04805.

Fleiss, J.L., 1971. Measuring nominal scale agreement among many raters. Psychological Bulletin 76, 378–382. https://doi.org/10.1037/h0031619

Keerthi, S.S., Shevade, S.K., Bhattacharyya, C., Murthy, K.R.K., 2001. Improvements to Platt's SMO algorithm for SVM classifier design. Neural computation 13, 637–649.

Li, H., Çelik, C., Bashir, M., Zou, L., Yang, Z., 2024a. Incorporation of a global perspective into data-driven analysis of maritime collision accident risk. Reliability Engineering & System Safety 249, 110187. https://doi.org/10.1016/j.ress.2024.110187

Li, H., Ren, X., Yang, Z., 2023. Data-driven Bayesian network for risk analysis of global maritime accidents. Reliability Engineering & System Safety 230, 108938. https://doi.org/10.1016/j.ress.2022.108938

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

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

Mao, R., Chen, G., Zhang, X., Guerin, F., Cambria, E., 2024. GPTEval: A Survey on Assessments of ChatGPT and GPT-4. https://doi.org/10.48550/arXiv.2308.12488

Maritime Cyber Attack Database (MCAD) | NHL Stenden university of applied sciences [WWW Document], 2025 URL https://www.nhlstenden.com/en/maritime-cyber-attack-database (accessed 1.10.25).

Mohsendokht, M., Li, H., Kontovas, C., Chang, C.-H., Qu, Z., Yang, Z., 2025. Enhancing maritime transportation security: A data-driven Bayesian network analysis of terrorist attack risks. Risk Analysis 45, 283–306. https://doi.org/10.1111/risa.15750

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

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

Raffel, C., Shazeer, N., Roberts, A., Lee, K., Narang, S., Matena, M., Zhou, Y., Li, W., Liu, P.J., 2023. Exploring the Limits of Transfer Learning with a Unified Text-to-Text Transformer. https://doi.org/10.48550/arXiv.1910.10683

Söner, Ö., Kayisoglu, G., Bolat, P., Tam, K., 2023. Cybersecurity risk assessment of VDR. The Journal of Navigation 76, 20–37.

Tam, K., Jones, K., 2019. MaCRA: a model-based framework for maritime cyber-risk assessment. WMU Journal of Maritime Affairs 18, 129–163.

Touvron, H., Lavril, T., Izacard, G., Martinet, X., Lachaux, M.-A., Lacroix, T., Rozière, B., Goyal, N., Hambro, E., Azhar, F., Rodriguez, A., Joulin, A., Grave, E., Lample, G., 2023. LLaMA: Open and Efficient Foundation Language Models. https://doi.org/10.48550/arXiv.2302.13971

Wei, J., Wang, X., Schuurmans, D., Bosma, M., Ichter, B., Xia, F., Chi, E., Le, Q.V., Zhou, D., 2022. Chain-of-Thought Prompting Elicits Reasoning in Large Language Models. Advances in Neural Information Processing Systems 35, 24824–24837.

Wu, B., Yip, T.L., Yan, X., Mao, Z., 2020. A Mutual Information-Based Bayesian Network Model for Consequence Estimation of Navigational Accidents in the Yangtze River. The Journal of Navigation 73, 559–580. https://doi.org/10.1017/S037346331900081X

Xu, B., Guo, X., Ye, Y., Cheng, J., 2012. An improved random forest classifier for text categorization. J. Comput. 7, 2913–2920.