




REVIEW ARTICLE

Literature review on maritime cybersecurity: state-of-the-art

Hongchu Yu,^{1,2}  Qiang Meng,³ Zhixiang Fang,⁴ and Jingxian Liu^{1,2}

¹ School of Navigation, Wuhan University of Technology, Wuhan, China

² Sanya Science and Education Innovation Park of Wuhan University of Technology, Sanya, China

³ Department of Civil and Environmental Engineering, National University of Singapore, Singapore

⁴ State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, Wuhan, China.

Corresponding author: Hongchu Yu; Email: hongshuxifan8140@163.com

Received: 9 August 2020; **Accepted:** 3 May 2023; **First published online:** 6 June 2023

Keywords: maritime cybersecurity; cyber-incidents recognition; consequence assessment; risk mitigation

Abstract

Maritime cybersecurity has attracted increasing attention in industrial and academic scope, which may be relevant to the increasing cyber-incidents in the maritime shipping industry. This paper presents a critical review of publications related to cybersecurity in the maritime transportation industry, to explore the current research status and gaps, as well as to guide new probe avenues by employing bibliometric approaches. With the advantage of bibliometric methods, the research focus and evolution are conformed and visualised. Representative papers are reviewed together to demonstrate maritime cyber-threats recognition and categories, as well as potential consequence assessment and risk mitigation actions recommendation. This paper also created a detailed database that is comprised of attack form, occurring time, targets, purpose, as well as potential results and cost, which has been included in the Appendix and is fully portable and extendible.

1. Introduction

The shipping industry is the lifeblood of international trade and is of great importance in the import/export of manufactured goods and affordable food. Maritime cargo and passenger movements not only contribute to the annual gross domestic product of involved countries, but also provide a variety of jobs and support employment. The continuously expanding maritime trade necessitates an increase in the size, types and capacities of ships. The means of monitoring and managing massive ships on the ocean receive vital attention, which is essential for safety management and environment protection, such as reducing accidents and carbon dioxide emissions. With the harnessing of advanced technology, such as the deployment of Radio Detection and Ranging (RADAR), Automatic Identification System (AIS) and Electronic Chart Display and Information System (ECDIS), it is clear that information communication technology (ICT) facilitates the collection, storage, integration, transmission, exchange, display, analysis, fusion and application of maritime traffic and transportation information on the ship and ashore and on the water to improve and enhance navigation, operations and services to ensure security and safety at sea, as well as protecting the marine environment and ecosystem. However, adversely, ICT can result in significantly dangerous situations caused by cyber-incidents against the maritime transportation system via potential deliberate disruptions (Perrine et al., 2019). Therefore, it is vital to achieve powerful cybersecurity management, including deploying appropriate adversarial models, maintaining robustness risk frameworks and designing resiliency counterpart plans. For example, the situation

awareness for navigation must reach beyond the physical observation domain (i.e. collision risk evaluation and prediction, the effect of environmental conditions on collision risk) (Fang et al., 2018a; Yu et al., 2019, 2021a, 2021b, 2023; Xu et al., 2021, 2023; Liu et al., 2023) and the mutual dependability risk reconnaissance between cyber and physical systems.

Maritime cybersecurity emphasises the new vulnerabilities of the maritime domain introduced by utilising advancements in ICT, and relies on a comprehensive understanding of cybersecurity to navigate, operate and communicate securely and safely. Cybersecurity in the maritime transportation industry engages in the availability and integrity of the shipping system. It not only protects information transmission, storage and usage, but also security mesh network, facilities, hardware and software from malicious and unauthorised use. Recently, cyber-attacks show their power to affect the maritime domain through crossing borders and breaking down the normal physical–cyber interaction, and they have the power to create revenue losses and provoke accidents (i.e. collision and grounding, etc.) by manipulating sailing information. The synthetic framework to deal with cyber-attacks in the maritime transportation domain and ensure security in the shipping system is highly correlated with the process of threats recognition, attacks classification, consequence assessment and mitigation recommendation.

Preventing cyber-attacks is attracting increasing attention in the maritime transportation industry; for example, on 16 May 2019, the Maritime and Port Authority of Singapore (MPA) announced plans to create the Maritime Cybersecurity Operations Center (MSOC) to strengthen and enhance the maritime transportation cybersecurity posture for Singapore.¹ This will have the potential to allow the MPA to closely cooperate with various entities to protect critical information infrastructures based on investigating and learning from cybersecurity threats. The MPA also plans to establish critical data linkages between the Port Operations Control Centre and MSOC against cyber-incidents in a more holistic and timely manner. In addition, the ‘Ship Cyber Security Network Construction and Design Safety Evaluation’ was launched by the Marine Engineering Research Centre of Samsung Heavy Industries in cooperation with the Classification Society Korean Register to enhance ship cybersecurity.² However, the current research on maritime security in the academic area is unknown, and it is worth filling in this gap.

This paper aims to highlight the necessity and importance of maritime cybersecurity. Section 2 presents the data collection and the bibliometric approach used for this paper. Section 3 first presents a brief review of evaluation of potential consequences of a cyber-attack, focusing on which methodologies are applicable to analyse the impact for the different cyber-attack types considered. Second, a brief summary of maritime cyber-threats is provided, centring on the question of how maritime cyber vulnerabilities can be recognised from different perspectives. Then, the classification of cyber-attacks to the maritime industry is presented, including implications for convincing evidence that have been considered in cyber-attack risk analysis and extended uncertainty treatment. Fourth, a recommendation of risk mitigation actions on the scope of the analysis in attack events and consequences is illustrated. Section 4 attempts to identify the research gaps that are closely connected with promising future research avenues. Section 5 presents the conclusion.

2. Data and bibliometric approach

Scopus is one of the largest topics, abstract, full paper and citations databases of peer-review literature, covering both journal and conference articles. Thus, for this study, publications are retrieved from the core collection of Scopus. A search with the key topics/keywords ‘maritime’ and ‘cybersecurity’ yielded numerous records. After refinement and careful inspection, closely relevant records with access to the full paper were eventually reviewed. The sources of the studies were diverse and *The Journal of Navigation* is one of the journals with voluminous publications available. According to the categories that Scopus assigns to the publications, the studies on maritime cybersecurity are dominated by Engineering (57.44%), Social Science (40.43%) and emerging Computer Science (38.80.18%). The number of

¹<https://www.mpa.gov.sg/web/portal/home/media-centre/news-releases/detail/8a5114cf-8214-4b46-8999-2c6c42433b1e>

²<https://www.hellenicshippingnews.com/korean-register-signs-cybersecurity-agreement-with-samsung-heavy-industries/>

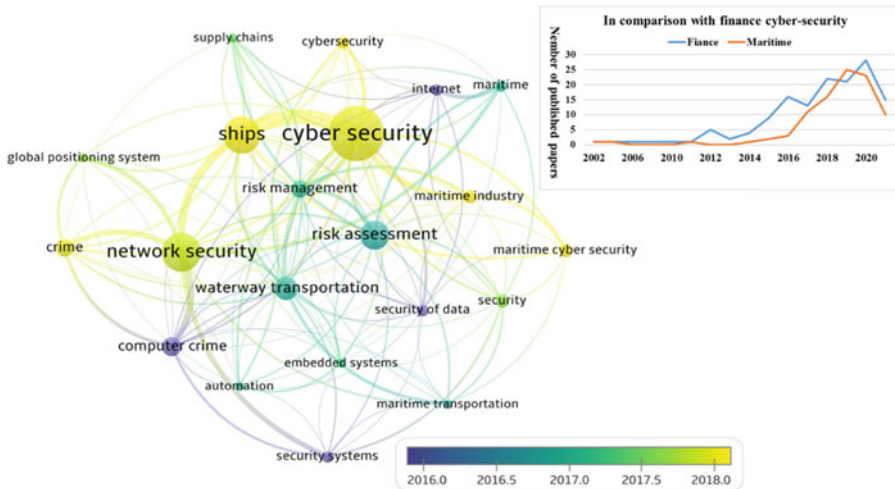


Figure 1. Keywords co-occurrence analysis.

publications associated with the keywords before 2015 is surprisingly low (17.65%), but the topics appear to have had explosive growth beginning in 2015. That indicates that maritime cybersecurity has gained increasing attention recently and is a hot topic nowadays.

The keywords co-occurrence analysis based on VOSviewer Software³ is meant to detect research hotspots, as shown in Figure 1. The node size illustrates the appearance times of a specific keyword, and the width of links represents the number of papers in which the connected two keywords co-occur. The different colours indicate different clusters where keywords are more likely to occur together, as well as the evolution over time. Obviously, maritime cybersecurity has attracted attention since 2016, and especially after 2018, cybersecurity, ships and network security are more possible to link simultaneously. In comparison with cybersecurity studies in the finance areas, the study on cybersecurity of the maritime transportation system started later but has similar trends in the number of published papers. Impactful studies with more citations are continuously conducted and developed; for example, studies on maritime cyber security with more citations are increasing. A series of solid research studies are essential to figuring out the core problems and corresponding detailed solutions within each step of the maritime system operation (Figure 1).

3. Major research focuses and trends

3.1. Potential consequence of maritime cyber-threats

Cyber-attacks have the power to destroy maritime navigation systems partly or totally on a port, regional and global scale. The potential consequences derived from cyber-attack incidents are involved in sea navigation and routing, port operation, shipping systems, and network, etc. (Jones et al., 2016; Hemminghaus et al., 2021). Some of the studies explained the consequence from the theoretical analysis perspective. Some relevant examples are mentioned here. DiRenzo et al. (2015) stated that these attacks may control the navigation system of ships using false signals that overpower authorised signals, triggering false collision warnings by creating images of fake ships that were recognised as real; tilting an oil rig, forcing it to shut down; or releasing cargo to false trucks and stealing the cargo without the port's knowledge. These are examples are based on theoretical results of incidents, however solid impact-consequence assessment models and their potential solutions are missing. Spousta and Chan (2016) asserted that buoys data under cyber-manipulation enable false impending tsunami announcements and even breach electric power systems through contextualising the connection between the buoy

³<https://www.vosviewer.com/>

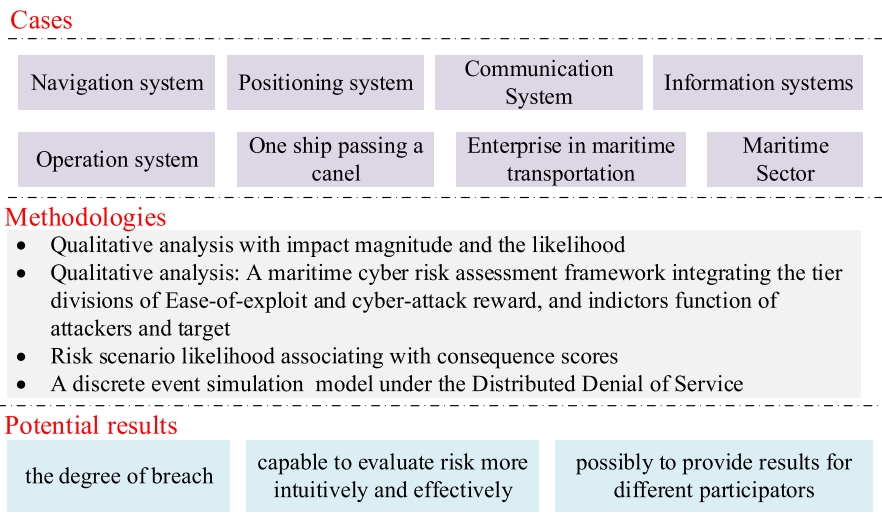


Figure 2. *Statistics of potential consequence assessment in the maritime cybersecurity domain.*

data, transmission network, warning system and infrastructure resilience. Shapiro et al. (2018) discussed the actors, intention, tactics and targets of the Trojan Horse virus, explaining the dangers for maritime sectors exposure to this threat from the perspective of personnel, computer system and the physical environment, and advised a variety of safety and security measures for risk mitigation and emergency management.

Other methodologies have tried to assess consequences from the qualitative perspective, including impact magnitude and the likelihood of vulnerabilities (Svilicic et al., 2019a, 2019b, 2019c, 2019d; Meland et al., 2022), a maritime cyber-risk assessment framework integrating the tier divisions of attackers and targets (Tam and Jones, 2019a), risk scenario likelihood associated with consequence scores (Abkowitz and Camp, 2011) and a discrete-event simulation (Bou-Harb et al., 2017) model under a distributed denial of service. These methods enable the evaluation of risk more intuitively and effectively; nevertheless, the risk assessment mostly focuses on the direct degree of vulnerabilities in maritime cyber systems and it is hard to estimate the actual real impact in the physical shipping industry, for example with economic loss and indirect impacts throughout sea routing and the whole shipping network. A fruitful consequence assessment must focus more on the larger impact of cyber-attacks rather than on localised effects. The accurate risk values for maritime cyber-attacks are unavailable beforehand, and can only be modelled based on the data of an accessible incident. Thus, the construction of the incidents database is meaningful and useful. In addition, they mixed some qualitative and subjective analyses; for example, the limited description for considered scenarios, the division of the level in the scoring process highly relies on participants, and the quality-control relative to empirical data is important for the reasonableness of results. Furthermore, extending the proposed model to diverse maritime security cases, comparison among different models and providing resiliency mechanisms is the intention of future work for the safe maritime operation (Figure 2).

3.2. *Recognising maritime cyber-threats*

The maritime shipping system consists of people, facilities, equipment, technology, information and networks that are intertwined and interactive. It is the resultant complexities and sophistication that make it challenging to protect maritime transportation from cyber-attacks. Maritime cyber-attack reconnaissance is the most important phase, which informs us that one attacker will pursue whatever means available to obtain vital information about targets in the maritime transportation system. Cyber-threat

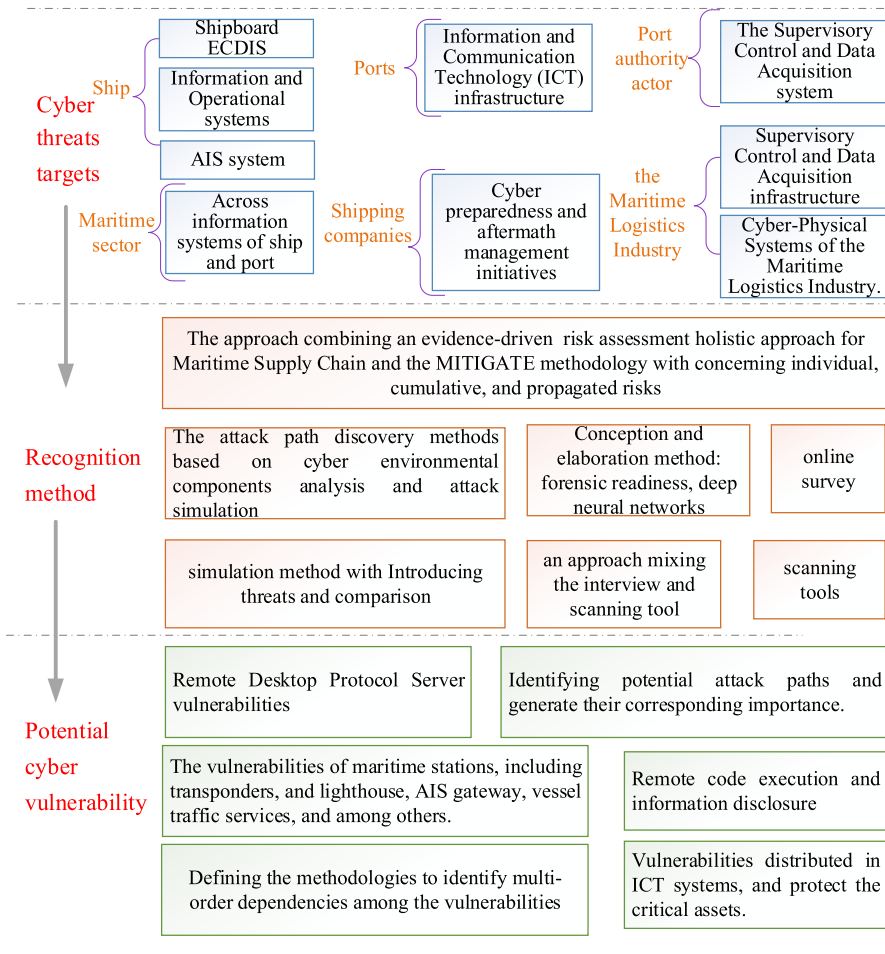


Figure 3. Statistics of maritime cyber threats recognition.

recognition is closely linked to a comprehensive understanding of the entire configurations of the maritime transportation system. A potential cyber-attacks vector of the maritime transportation system can be obtained based on in-depth knowledge of operational, communicational and technical aspects of such a system. Figure 3 summarises the cyber-attacks recognition in the view of the ship, port, maritime sector, shipping companies and logistics industry.

Ships and ports are the central roles of maritime transportation with several shipboard navigation systems, such as ECDIS and AIS, as well as Voyage Data Recorder (VDR), providing real-time sailing information to ensure safety and efficiency (Söner et al., 2023). Meanwhile, the number of ship- and port-involved cyber-attacks (Silverajan et al., 2018) has increased, using such instruments as code injection, tampering and modification, GPS and AIS spoofing, signal jamming and information eavesdropping, as well as link disruption, which can utilise one or several vectors, such as a positioning system, firmware, sensors, VDRs, intra-vessel networks, vessel-to-shore communications, remote operation systems and so on. The cyberattack vectors in shipping companies and the maritime logistics industry are close to the ships and ports; thus, the cyber-risk recognition method is an alternative for increasing protection against cyber-attacks.

In order to identify the potential cyber-risks from this embedded software, the recognition approaches can be grouped into scanning tools, online surveys, participators interviews, introducing threats and simulation, conception and elaboration method and attack graph generation, as well as the cyber-attack

path discovery method (Balduzzi et al., 2014; Kalogeraki et al., 2018b; Lee and Wogan, 2018; Möller et al., 2018; Mouratidis and Diamantopoulou, 2018; Polatidis et al., 2018; Jacq et al., 2019a; Tam and Jones, 2019b). For example, we can use the industry-leading vulnerability scanning tool (i.e. Nessus Professional Version) to detect weak components (Svilicic et al., 2019e) in a system. The threats can be derived from out-of-date and unsecured setup and bad health of the underlying operating system, insufficient training and lack of awareness of navigational ranks, establishing unauthorised access to the internet connection, inability to continuously assess and respond rapidly to cyber-risk, and a lack of self-contained cybersecurity procedures and policies (Svilicic et al., 2019a).

However, there are several limitations that require further study. First, most of the current recognition research based on cyber-threats and cyber-assets will be problematic without considering physical and cyber interaction. Second, most of these approaches are theoretical solutions, and they lack practical implementation and considering privacy requirements. The validation as proof for application of real cyber-attack scenarios is missing. Third, the studies are limited to application in the real port and supply-chain cyber-risk assessment without incorporating the physical nature of infrastructure on cyber-risk estimation reasoning, results and potential cascading effects, as well as incident management practices. Finally, further research is required regarding cyber-attacks predictions integrating vulnerabilities, attack paths, the importance of assets, previous attack incidents database and the possibility of exploiting mitigation recommendation methods and defence strategies.

3.3. *Categorising the maritime cyber-risk*

Increased digitalisation, automation and informatisation in maritime transportation appears to open a new gateway of vulnerability for shipping systems concerned with cybersecurity. There are few differences between maritime cyber-attacks and general information-security threats, including worms, viruses and other types of malware, as well as email scams. The information technology system in maritime transportation has suffered from an increasing number of ongoing cyber incidents, as a result affecting operators, ports and shipping companies. In most of these cases where the shipping industry is a direct target of cyber breaches, they were sometimes affected by threats to other perspectives; for example, the NotPetya⁴ aimed at destroying an Iranian nuclear centrifuge, posing a breakdown of servers and computers of the Maersk Line. In addition, the components of the maritime shipping industry are not self-contained units, being linked with each other. An obvious example is that ship-based and shore-based information technology systems are cyber-connected, which opens the door to a cyber-attack reaching the critical operating technology systems of a vessel via shore-based information systems, resulting in troubling accidents. This type of threat could also penetrate the entire fleet system and spread quickly, causing devastating and costly consequences across the fleet.

Maritime cyber-risks can be classified into maritime transportation business disruption and maritime system execution failure, maritime data breach, theft or manipulation or loss of maritime information, theft or loss of funds from maritime sectors, and theft or loss of cargoes based on cyber-incident consequences (Curti et al., 2019). The exemplified cyber-incidents are shown in Figure 4, and the detailed description and source link are illustrated in the Supplementary Materials. Cybercriminals can target the servers and computers of shipping companies, cargo management systems, the movement controlling and locating system, the customer service system, shipboard network and the positioning system, among others. Each component of electronic communications is vulnerable to cybercriminal attack. The purposes of cybercriminal activity can be to track illegal cargoes and reroute them away from custom checking, producing fake bills to steal cargo and defraud money, infiltrating some information systems and stealing confidential data to request ransom payment, and disrupting internal administrative functions and destroying continuous operations, as well as diverting deliveries of unmanned ships. Cyber-incidents are mostly aimed at gaining profit from shockwaves among maritime transportation systems or increasing costs for the shipping industry.

⁴www.scmagazine.com/notpetya-attack-totally-destroyed-maersks-computer-network-chairman/article/739730/

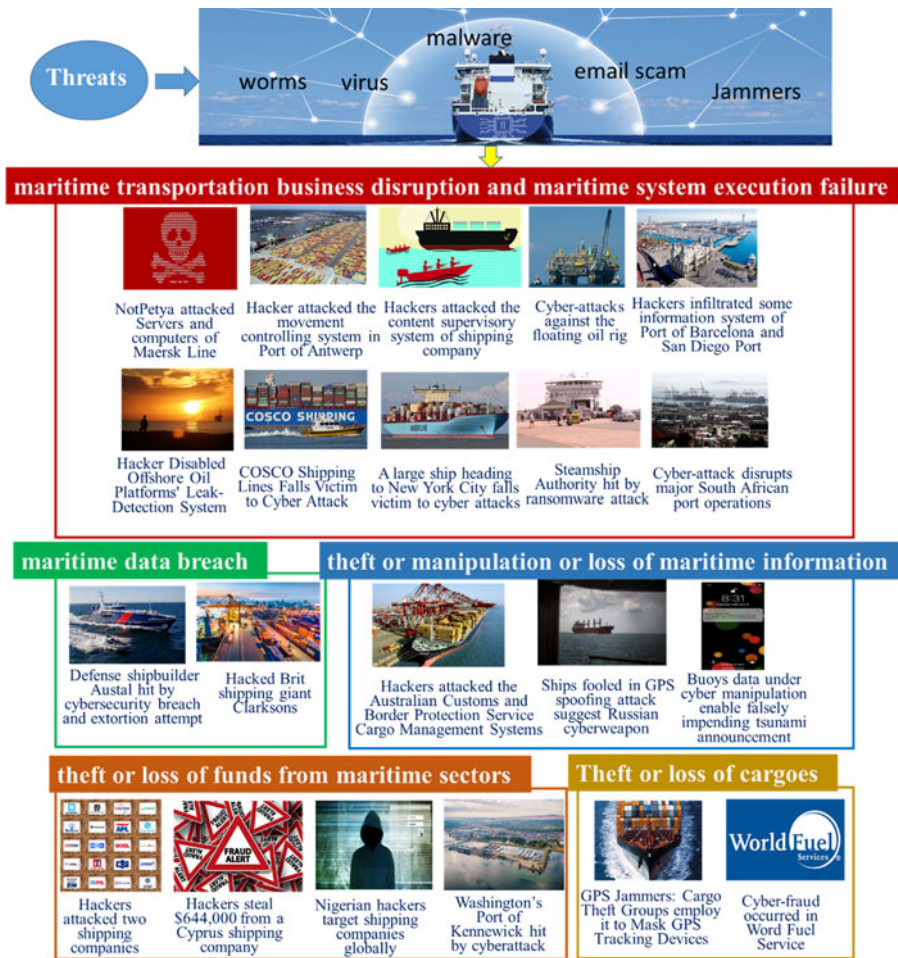


Figure 4. Exemplified cyber-incidents.

Another attack method is denial-of-service to prevent authentication access to the official system. Most of the GPS-spoofing instances appear around sensitive regions in Crimea and Russia during the periods when presidents and high-ranking officials were presented. These attacks emphasise the weakness and vulnerability of AIS because the widespread disruption for a huge number of ships causes navigation difficulties and changes in course, perhaps even collision accidents in congested waters. Questions of how to detect such attacks and prepare for the denial-of-service and develop countermeasures based on the big AIS movement data are worth exploring. The detailed database for maritime cyber incidents is included in the Supplementary Material, including the attack form, time of occurrence, targets, purpose, and potential results and costs, which are fully portable and extendible, and meaningful to further research incorporating real accident data.

3.4. Mitigating maritime cyber-risk

Scholars, industry experts, and government and municipal authorities have jointly advocated for more solid cybersecurity checks and balances in every part of the maritime system, navigator competency enhancement (Hareide et al., 2018; Akpan et al., 2022) to recognise and deal with cyber-attacks appropriately, and a build-up of synthetic reliable systems, including raising awareness of cybersecurity, improving the competence of involvers, maintaining robustness risk estimation framework, deploying

confrontational methodologies and models, and designing flexible counterpart plans (Amro and Gkioulos, 2022). It is essential to develop the incentive to actively collect cyber-attacks evidence with scrutiny of every part of the maritime shipping industry under every minor or significant threat. This requires in-depth actions at multiple levels, such as policy, technical, training, enforcement and implementation.

With respect to crews, raising awareness and training about cyber-attacks for crews can be an important solution to mitigate maritime cyber-risk. Vigilant seafarers who become highly situational aware and make wise navigation decisions onboard ships can be the most important asset for maritime security (Spidalieri and McArdle, 2016; Hareide et al., 2018; Lund et al., 2018b; Thant, 2018; Jacq et al., 2019b; Pseftelis and Chondrokoukis, 2021; Tam et al., 2021a; Kayisoglu et al., 2022; Hopcraft et al., 2023; Potamos et al., 2023). Conversely, the seafarers' lack of competence and system awareness will present risk factors rather than risk reductions (Heering et al., 2020). The holistic framework to increase cybersecurity awareness and competence of seafarers includes theoretical education and practical training, and demonstrations and experiments, as well as assistance procedure development of identifying and dealing with cyber threats (Becmeur et al., 2017; Zăgan et al., 2018; Lovell and Heering, 2019; Tam et al., 2021b). The cross-sector capacities in the overlapping domains of automation, digital system, robotic, artificial intelligence, cyber, maritime shipping and navigation are the skills requirements for intelligent maritime shipping (Harris, 2021). Thus, the introduction of training for these key technologies means that various combinations of professional and interdisciplinary courses are essential in all short-, medium- and long-term cyber-security training of mariners.

In the case of ships, the protections and risk mitigations are comprised of controlling access to the shipboard network; limiting unauthorised personnel to access the information operation system, such as enforcing per-user accounts and passwords; adhering to security protection procedures; and timely updating of installed software for the ships and patching regularly, among others options. The owner of the vessels can extend cooperation with anti-cyber-attacks companies, such as Gatehouse Maritime and James Fisher Mimic, to invest and develop cyber-surveillance products and release a set of efficient patches to monitor, inspect, find and respond to suspicious incursions and to build solid firewalls to recognise and detect anomalies that are essential for early alert and avoiding serious impacts. Another important part of cyber-risks understanding and cyber-incidents detection is forming the forensic readiness of ships for seafarers' training and management, as well as developing secure evidence-handling measures.

In the case of shipping companies, they must carry out regular cybersecurity assessments for their information management system to identify new security weaknesses and breaches, and install corresponding patches. This requires scrutiny in checking that the vessels are operated with a contracted crew formed from multiple layers of outsourcing to track assigned responsibility for the information technology system. Ship companies should introduce uniform security standards for technology, payment, organisation, analytics and automation (i.e. International Organization for Standardization, etc.) to decrease friction and enable communication between various cyber-risk control actions activated by different security platforms and products, as well as embrace ships, terminals, ports and stakeholders, forming coordination across the entire industry (Jensen, 2015). Most importantly, ship companies should be more proactive in assessing and responding to any risks in cybersecurity, no matter how minor or impactful. Finally, cybersecurity awareness and cyber-hygiene, as well as cyber-incident training for the personnel of the shipping company, is vital for avoiding or abating the damage of cyber-threats to shipping operations.

Regarding the shipping industry regulation, the maritime safety committee of the International Maritime Organization (IMO) released Resolution MSC-FAL.1 and MSC.428 (98) in June 2017, implemented in January 2021, to introduce measures to tackle cyber-risks in maritime safety supervision and management systems, and cyber-code has potential as a binding instrument to assure the security and improve the efficiency of the maritime industry in confronting cyber-attacks (Hopcraft and Martin, 2018). The new legislation will likely be ongoing to make sure that only vessels with the cybersecurity certificate issued by authorising institutions are allowed to operate and sail on marine.

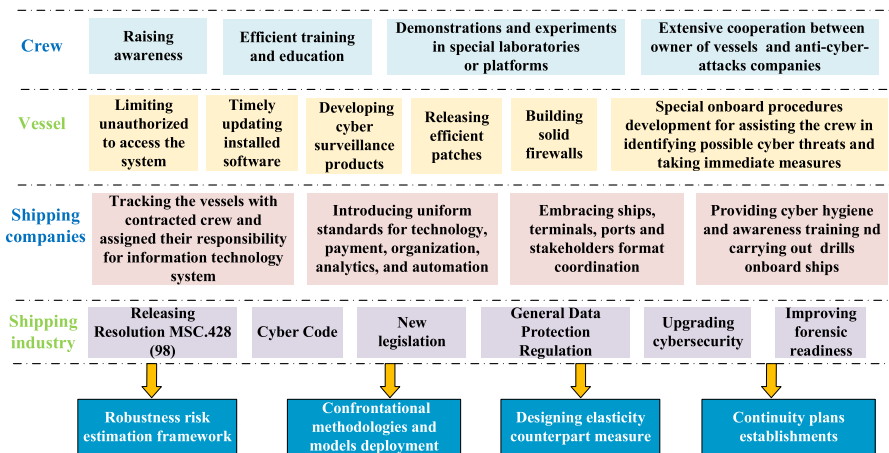


Figure 5. Risk mitigation recommendation.

The General Data Protection Regulation can also be applied to regulate the storage and processing of shipping data, for example providing data with the consent subjects rather than giving freely. Furthermore, backend databases must be queried weekly to identify new suspicious data according to malicious records. The maritime transportation industry should upgrade cybersecurity in accordance with advances in technology and information communication, such as integrating experts in cybersecurity products, devices, and services, as well as data protection. Moreover, the maritime cybersecurity management certification system should be built in the maritime industry to provide certification services for ships, ports, companies, shipping networks and communication systems. These can help the maritime industry to better prepare for serious cyber-attacks and develop counterattack strategies quickly, decreasing costs successfully.

Establishment of appropriate continuity plans is essential for countermeasures targeting cyber-incidents. That means that even though the worst event occurs, the maritime transportation system can continue to operate by utilising alternative modes and subsystems. That means applying the principle of creating maritime shipping system layers with independent information communication levels, to ensure the reliability of the transportation system. In order to counter the loss of critical systems, the standardisation of information transmission and interfaces and operations enabling integrate navigation and communications is meant to duplicate key components and strategy development. Frøystad et al. (2017) believed that public key infrastructure solutions can protect future maritime domains through the introduction of authentication and cryptograph systems into the communication between ship and ship, as well as between ship and shore. However, the international trust hierarchy establishment requires a huge amount of both technical and political effort, and it may be the ongoing process after the standardisation achievement of worldwide maritime communication in the future (Figure 5).

3.5. Research gaps and promising avenues

Digitalisation and information integration will enhance the operational efficiency through earlier visibility regarding the transport modality of each ship, better yard planning for rail ports and heavy trans-shipment, and online management of logistics. However, the risk to the maritime shipping industry to cyber-attacks is rising as quickly as such solutions and defences are created. Cyber-attacks can be delivered inexpensively and from any place, which means it is almost impossible to detect and trace, but can cause serious damage. The goal of cybersecurity situational awareness and comprehension is to successfully recognise cyber-attacks, underline origins and causality, and assess potential consequences and impacts, as well as predict and project vulnerabilities in the future. Current works generally focus on analysis involved with simple cyber-attacks through concept methods, qualitative analysis and simple

scenario-driven simulations. However, deeper and more sophisticated analysis is required to deal with complex attacks. For example, the technology and methodology are enabled to create the timeline of cyber-attack events based on search and mining over a huge amount of spatiotemporal heterogeneous information. It is worth mentioning that the principles of the graph and complex network theories are valuable to figure out streamlines and pivots among the linked information (Fang et al., 2018b).

Researchers have tried to examine the cyber-attack incidents statistics, responsibility division, and counterpart strategy recommendation through a qualitative elaboration approach. Mraković and Vojinović (2019) described the connectivity between the components in the systems of a ship and advocate the adequate proactive framework to solve onboard cybersecurity problems by integrating situation awareness, building competence, and solidification, and prediction to turn the conceptual framework into practical applications. Daum (2019) and Karim (2022) emphasised that the legal environment should keep pace with various advances in the cybersecurity domain of maritime shipping, including duty and sanction catalogue clarification. The IOM guidelines and regulations with specific and detailed maritime cybersecurity actions are precedents and predecessors for legislation and amendments. The complement of the legal environment may be realised in the near future. Ahvenjärvi et al. (2019) discussed safe information exchange considering type, characteristic, mode and role, however they are still formulating the relative contents, as with the cybersecurity incidents sharing among navigation systems reported by Silverajan and Vistiaho (2019). Maritime cybersecurity is confronted with numerous challenges from the perspectives of legislation and technology and implementation. All technological loopholes declassification and their impacts on the entire shipping systems evaluation are outside the scope of the existing research.

With respect to the abuse of AIS data, the means to detect these anomalies, deter the false sentences forwarding to official and navigational pages, and recover the true information and transmission are currently unknown. Perhaps the various popular machine-learning technologies can be applied to recognise anomalies and asymmetric cryptography works to protect the AIS data (Botunac and Gržan, 2017). The cryptographic countermeasures will increase one layer of safety, including a key-pair of security (signature with private key and verification by the corresponding public key) and the specialised identity-based signature strategy (the public key with identity and no need to certificate) (Lund et al., 2018a). Data encryption based on implementing advanced encryption standards and algorithms (i.e. Truecrypt, Blowfish) is the option for making maritime data acquisition systems more resilient. In addition, incorporating the multi-source data to generate the alternative results and cross-referencing the veracity with the ability to detect anomaly driven by the application of Big Data Paradigm could also be a potential future maritime security enhancement (Spousta and Chan, 2016).

In addition, there is an essential shift from analysing the concept model of the maritime cybersystem to the real system, which requires defining the challenges and complex interdependencies instead of heavily relying on the instrumentation and functional block and unified modelling diagrams. Polemic and Papastergiou (2015) elaborated the MITIGATE project (Kalogeraki et al., 2018a) evolution from CYSM and MEDUSA to define the methodologies used to identify multi-order dependencies among the vulnerabilities of cyber-assets and cyber-threats covering the multi-sector cross-border simulation scenarios to guide security knowledge representation; however, this is limited to application in the real port and supply-chain cyber-risk assessment without incorporating cyber-risk estimation reasoning results and potential cascading effects. The synergy of physical and computational components is the true way to develop the modern physical–cyber system (Tam et al., 2021a). That indicates that more research is needed in this direction. Undoubtedly, we endeavour to conquer significant challenges to achieve the envisioning goals that pinpoint tangible maliciousness and provide resilience and security of maritime transportation, despite that fact that many factors, including lack of sufficient empirical data working for capturing, inferring, analysing maritime cyber-attacks, and hard-to-access obvious diversity of cyber–physical controlling and operating systems with complete and elaborative technical details that are related to privacy constraints enforced by maritime shipping and logistics.

The development of a blueprint for maritime cybersecurity training of ship crews and managers can be as important as the technical solutions. The workbook and guidelines published by IMO, the

International Chamber of Shipping, the International Union of Marine Insurance and others can provide some support and guidance. However, there are some significant challenges that the maritime shipping sector must overcome in the nearest future for the cybersecurity training of crews. First, the collaboration between the educational institution and the shipping sector must be enhanced to ensure that there exists an adequate number of institutions to provide ship officers with specific cybersecurity education. Second, the International Convention on Standards of Training, Certification, and Watch-Keeping for Seafarers (STCW) should include a requirement for cybersecurity education and provide guidelines for the development of study materials in various native languages (Kidd and McCarthy, 2019). Third, the bachelor's and master's programs on water navigation in the maritime university should include cybersecurity courses that are comprised of theoretical cybersecurity knowledge and practical exercises based on simulators and cyber-attack vectors. The curriculum of maritime education and training methods of maritime professionals should keep up with technological innovation and prepare for future unmanned ships (Yamada, 2020).

4. Conclusion

With the increasing standardisation, informatisation, efficiency and automation of shipping systems, the systems seem to lose robustness proportionally, especially for cyber-attacks, and become vulnerable to small internal and external mistakes or impacts. The modernisation and robustness proceed in opposite directions in the maritime system. In other words, the current complicated maritime system is susceptible to disturbances and errors. Especially with the development of remote control technology and unmanned surface vehicles, experienced mariners will control and operate the autonomous vessel from state-of-the-art onshore facilities through satellite communications instead of through actual people on board. Therefore, maritime cybersecurity is vital in the current maritime industry. Participants take steps and actions to preserve servers, computers, control systems, communication systems, digital equipment and other components from stakes associated with insufficient cybersecurity.

Currently, maritime cyber-threats recognition and potential consequence assessment are mainly based on the conceptual model, theoretical framework, designation graph, qualitative methods and simulation, and thus quantitative methodologies are in great demand to fully consider physical and cyber interaction on cyber-risk estimation, reasoning results, potential cascading effects assessment and incident management practices. Maritime cyber-risk analysis, modelling and predicting are multiple-discipline domain research questions that require input from computer science, shipping agents, port authority, seafarers, technology management and others. Human knowledge, technology, and legislation are the primary pillars with respect to the cybersecurity process. Human training and education and legislation are ongoing processes. These are still great opportunities that encourage scholars from multiple disciplines to contribute to the related cybersecurity studies.

Alleviation of the cyber-risks and reduce cyber-incidents, the cyber-risk assessment toolkit that enables researchers to model cyber properties and interactions, analyse the dependencies among threats, identify vulnerabilities and disruption level, detect possible contingency requirement, determine and deploy safety countermeasures, as well as provide intuitive and interactive tools to represent, organise, and management all cybersecurity contents, is the central technology part of the collaborative security management and risk prevent system (Karantjias et al., 2014; Papastergiou and Polemi, 2014, Chiappetta and Cuzzo, 2017). There are still numerous challenges to turn the concept into practice, such as the visualisation and analysis of the dependencies among business entities-based designation graphics, making it hard to reflect the interconnected assets. The collaborations among the cybersecurity management system foster the interaction and communication among different ports and all the operators and navigators to share and distribute information, knowledge, experience, skills and expertise. This communication and interaction can raise the cybersecurity awareness and culture and draw a more digital safety practice-aid strategy for the involved stakeholders. For example, the visualisation of vulnerabilities and risks offers quick and intuitive risk value and erroneous characteristics. Meanwhile, it will assist operators and managers to behave in compliance with the legislation and

regulations. Maritime cybersecurity research is a multidisciplinary question that is worth cooperation among network security, maritime shipping, information communication and internet security entities.

Supplementary material. The supplementary material for this paper can be found at <https://doi.org/10.1017/S0373463323000164>.

Acknowledgements. This work was supported in part by the National Natural Science Foundation of China, No. 42101429; Open Fund of State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University (Grant No. 21S04), Fund of Sanya Science and Education Innovation Park of Wuhan University of Technology (Grant No.2021KF0026), the National Key Research of China, 2022YFC3302703, and the Young Elite Scientists Sponsorship Program by China Association for Science and Technology (CAST) (No. YESS20220491).

Competing interests. The authors declare that they have no known competing financial interests or personal relationships that could have occurred to affect the research reported in this paper.

References

- Abkowitz, M. D. and Camp, J. S. (2011). An application of enterprise risk management in the marine transportation industry. *WIT Transactions on The Built Environment*, **119**, 221–232.
- Ahvenjärvi, S., Czarnowski, I., Kåla, J., Kyster, A., Meyer, I., Mogensen, J. and Szyman, P. (2019). Safe information exchange on board of the ship. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, **13**, 165–171.
- Akpan, F., Bendiab, G., Shialeles, S., Karamperidis, S. and Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. *Network*, **2**(1), 123–138.
- Amro, A. and Gkioulos, V. (2022). From Click to Sink: Utilizing AIS for Command and Control in Maritime Cyber Attacks. In *Computer Security–ESORICS 2022: 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26–30, 2022, Proceedings, Part III*. Cham: Springer Nature Switzerland, pp. 535–553.
- Balduzzi, M., Pasta, A. and Wilhoit, K. (2014). A Security Evaluation of AIS Automated Identification System. In *Proceedings of the 30th Annual Computer Security Applications Conference*, pp. 436–445.
- Becmeur, T., Boudvin, X., Brosset, D., Héno, G., Merien, T., Jacq, O., Kermarrec, Y., and Sultan, B. (2017). A Platform for Raising Awareness on Cyber Security in A Maritime Context. In *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, pp. 103–108.
- Botunac, I. and Gržan, M. (2017). Analysis of software threats to the automatic identification system. *Brodogradnja: Teorija i praksa brodogradnje i pomorske tehnike*, **68**(1), 97–105.
- Bou-Harb, E., Kaisar, E. I. and Austin, M. (2017). On the Impact of Empirical Attack Models Targeting Marine Transportation. In *2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*. IEEE, pp. 200–205.
- Chiappetta, A. and Cuzzo, G. (2017). Critical Infrastructure Protection: Beyond the Hybrid Port and Airport Firmware Security Cybersecurity Applications on Transport. In *2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*. IEEE, pp. 206–211.
- Curti, F., Gerlach, J., Kazinnik, S., Lee, M. and Mihov, A. (2019). Cyber Risk Definition and Classification for Financial Risk Management. Federal Reserve Bank of St Louis, August. Mimeo.
- Daum, O. (2019). Cyber security in the maritime sector. *Journal of Maritime Law and Commerce*, **50**(1), 1–19.
- DiRenzo, J., Goward, D. A. and Roberts, F. S. (2015). The Little-Known Challenge of Maritime Cyber Security. In *2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA)*. IEEE, pp. 1–5.
- Fang, Z., Yu, H., Ke, R., Shaw, S. L. and Peng, G. (2018a). Automatic identification system-based approach for assessing the near-miss collision risk dynamics of ships in ports. *IEEE Transactions on Intelligent Transportation Systems*, **20**(2), 534–543.
- Fang, Z., Yu, H., Lu, F., Feng, M. and Huang, M. (2018b). Maritime network dynamics before and after international events. *Journal of Geographical Sciences*, **28**, 937–956.
- Frøystad, C., Bernsmed, K. and Meland, P. H. (2017). Protecting Future Maritime Communication. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, pp. 1–10.
- Hareide, O. S., Jøsok, Ø, Lund, M. S., Ostnes, R. and Helkala, K. (2018). Enhancing navigator competence by demonstrating maritime cyber security. *The Journal of Navigation*, **71**(5), 1025–1039.
- Harris, J. (2021). Future Skills Requirements for a Global Centre of Maritime Training and Education: Skills Challenges for the Solent. (Doctoral dissertation, Centre of Maritime Training and Education: Skills Challenges for the Solent Dr Jack Harris and Professor Peter Sunley, School of Geography and the Environment, University of Southampton).
- Heering, D., Maennel, O. M. and Venables, A. N. (2020). Shortcomings in Cybersecurity Education for Seafarers. In *5th International Conference on Maritime Technology and Engineering*, Lisbon, Portugal.
- Hemminghaus, C., Bauer, J. and Padilla, E. (2021). BRAT: a BRidge Attack Tool for cyber security assessments of maritime systems. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, **15**, 35–44.

- Hopcraft, R. and Martin, K. M. (2018). Effective maritime cybersecurity regulation—the case for a cyber code. *Journal of the Indian Ocean Region*, 14(3), 354–366.
- Hopcraft, R., Tam, K., Misas, J. D. P., Moara-Nkwe, K. and Jones, K. (2023). Developing a maritime cyber safety culture: improving safety of operations. *Maritime Technology and Research*, 5, 1.
- Jacq, O., Brosset, D., Kermarrec, Y. and Simonin, J. (2019a). Cyber Attacks Real Time Detection: Towards A Cyber Situational Awareness for Naval Systems. In *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)*. IEEE, pp. 1–2.
- Jacq, O., Laso, P. M., Brosset, D., Simonin, J., Kermarrec, Y. and Giraud, M. A. (2019b). Maritime Cyber Situational Awareness Elaboration for Unmanned Vehicles. In *Maritime Situational Awareness Workshop*.
- Jensen, L. (2015). Challenges in maritime cyber-resilience. *Technology Innovation Management Review*, 5(4), 35.
- Jones, K. D., Tam, K. and Papadaki, M. (2016). Threats and Impacts in Maritime Cyber Security.
- Kalogeraki, E. M., Apostolou, D., Polemi, N. and Papastergiou, S. (2018a). Knowledge management methodology for identifying threats in maritime/logistics supply chains. *Knowledge Management Research & Practice*, 16(4), 508–524.
- Kalogeraki, E. M., Papastergiou, S., Mouratidis, H. and Polemi, N. (2018b). A novel risk assessment methodology for SCADA maritime logistics environments. *Applied Sciences*, 8(9), 1477.
- Karantjias, A., Polemi, N. and Papastergiou, S. (2014). Advanced Security Management System for Critical Infrastructures. In *IISA 2014, The 5th International Conference on Information, Intelligence, Systems and Applications*. IEEE, pp. 291–297.
- Karim, M. S. (2022). Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat? *Marine Policy*, 143, 105138.
- Kayisoglu, G., Bolat, P. and Tam, K. (2022). Evaluating SLIM-based human error probability for ECDIS cybersecurity in maritime. *Journal of Navigation*, 75(6), 1364–1388.
- Kidd, R. and McCarthy, E. (2019). Maritime education in the age of autonomy. *WIT Transactions on the Built Environment*, 187, 221–230.
- Lee, A. R. and Wogan, H. P. (2018). All at Sea: The Modern Seascape of Cybersecurity Threats of the Maritime Industry. In *OCEANS 2018 MTS/IEEE Charleston*. IEEE, pp. 1–8.
- Liu, Z., Zhang, B., Zhang, M., Wang, H. and Fu, X. (2023). A quantitative method for the analysis of ship collision risk using AIS data. *Ocean Engineering*, 272, 113906.
- Lovell, K. N. and Heering, D. (2019). Exercise Neptune: Maritime Cybersecurity Training Using the Navigational Simulators. In *5th Interdisciplinary Cyber Research Conference 2019*, p. 34.
- Lund, M. S., Gulland, J. E., Hareide, O. S. and Weum, K. O. C. (2018a). Integrity of Integrated Navigation Systems. In *2018 IEEE Conference on Communications and Network Security (CNS)*. IEEE, pp. 1–5.
- Lund, M. S., Hareide, O. S. and Jøsok, Ø. (2018b). An Attack on an Integrated Navigation System.
- Meland, P. H., Nesheim, D. A., Bernsmed, K. and Sindre, G. (2022). Assessing cyber threats for storyless systems. *Journal of Information Security and Applications*, 64, 103050.
- Möller, D. P., Jehle, I. A., Froese, J., Deutschmann, A. and Koch, T. (2018). Securing Maritime Traffic Management. In *2018 IEEE International Conference on Electro/Information Technology (EIT)*. IEEE, pp. 0453–0458.
- Mouratidis, H. and Diamantopoulou, V. (2018). A security analysis method for industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(9), 4093–4100.
- Mraković, I. and Vojinović, R. (2019). Maritime cyber security analysis—How to reduce threats? *Transactions on Maritime Science*, 8(01), 132–139.
- Papastergiou, S. and Polemi, N. (2014). Harmonizing Commercial Port Security Practices & Procedures in Mediterranean Basin. In *IISA 2014, The 5th International Conference on Information, Intelligence, Systems and Applications*. IEEE, pp. 292–297.
- Perrine, K. A., Levin, M. W., Yahia, C. N., Duell, M. and Boyles, S. D. (2019). Implications of traffic signal cybersecurity on potential deliberate traffic disruptions. *Transportation Research Part A: Policy and Practice*, 120, 58–70.
- Polatidis, N., Pavlidis, M. and Mouratidis, H. (2018). Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards & Interfaces*, 56, 74–82.
- Polemi, N. and Papastergiou, S. (2015). Current Efforts in Ports and Supply Chains Risk Assessment. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, pp. 349–354.
- Potamos, G., Theodoulou, S., Stavrou, E. and Stavrou, S. (2023). Building Maritime Cybersecurity Capacity Against Ransomware Attacks. In *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022*; 20–21 June; Wales. Singapore: Springer Nature Singapore, pp. 87–101.
- Pseftelis, T. and Chondrokoukis, G. (2021). A study about the role of the human factor in maritime cybersecurity. *SPOUDAI—Journal of Economics and Business*, 71(1-2), 55–72.
- Shapiro, L. R., Maras, M. H., Velotti, L., Pickman, S., Wei, H. L. and Till, R. (2018). Trojan horse risks in the maritime transportation systems sector. *Journal of Transportation Security*, 11(3-4), 65–83.
- Silverajan, B. and Vistiaho, P. (2019). Enabling Cybersecurity Incident Reporting and Coordinated Handling for Maritime Sector. In *2019 14th Asia Joint Conference on Information Security (AsiaJCIS)*. IEEE, pp. 88–95.
- Silverajan, B., Ocak, M. and Nagel, B. (2018). Cybersecurity Attacks and Defences for Unmanned Smart Ships. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, pp. 15–20.

- Söner, Ö., Kayisoglu, G., Bolat, P. and Tam, K. (2023). Cybersecurity risk assessment of VDR. *The Journal of Navigation*, First View, 1–18.
- Spidalieri, F. and McArdle, J. (2016). Transforming the next generation of military leaders into cyber-strategic leaders: the role of cybersecurity education in US service academies. *The Cyber Defense Review*, **1**(1), 141–164.
- Spousta, R. and Chan, S. (2016). Ocean Data Vulnerability to Cyber Manipulation and Consequences for Infrastructural Resilience. In *2016 Future Technologies Conference (FTC)*. IEEE, pp. 672–680.
- Svilicic, B., Rudan, I., Jugović, A. and Zec, D. (2019a). A study on cyber security threats in a shipboard integrated navigational system. *Journal of Marine Science and Engineering*, **7**(10), 364.
- Svilicic, B., Brčić, D., Žuškin, S. and Kalebić, D. (2019b). Raising awareness on cyber security of ECDIS. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, **13**, 1.
- Svilicic, B., Kamahara, J., Celic, J. and Bolmsten, J. (2019c). Assessing ship cyber risks: a framework and case study of ECDIS security. *WMU Journal of Maritime Affairs*, **18**(3), 509–520.
- Svilicic, B., Kamahara, J., Rooks, M. and Yano, Y. (2019d). Maritime cyber risk management: an experimental ship assessment. *The Journal of Navigation*, **72**(5), 1108–1120.
- Svilicic, B., Rudan, I., Frančić, V. and Doričić, M. (2019e). Shipboard ECDIS cyber security: third-party component threats. *Pomorstvo*, **33**(2), 176–180.
- Tam, K. and Jones, K. (2019a). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, **18**(1), 129–163.
- Tam, K. and Jones, K. (2019b). Forensic Readiness Within the Maritime Sector. In *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)*. IEEE, pp. 1–4.
- Tam, K., Hopcraft, R., Moara-Nkwe, K., Misas, J. P., Andrews, W., Harish, A. V., Giménez, P., Crichton, T. and Jones, K. (2021a). Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety. *Journal of Transportation Technologies*, **12**, 1–27.
- Tam, K., Moara-Nkwe, K. and Jones, K. (2021b). The use of cyber ranges in the maritime context: assessing maritime-cyber risks, raising awareness, and providing training. *Maritime Technology and Research*, **3**(1), 16–30.
- Thant, M. M. (2018). The Legal, Administrative and Operational Framework for the Safe Maritime Transport of Dangerous Goods: Myanmar as a Case Study.
- Xu, L., Chen, N., Chen, Z., Zhang, C. and Yu, H. (2021). Spatiotemporal forecasting in earth system science: methods, uncertainties, predictability and future directions. *Earth-Science Reviews*, **222**, 103828.
- Xu, L., Yu, H., Chen, Z., Du, W., Chen, N. and Zhang, C. (2023). Monthly ocean primary productivity forecasting by joint use of seasonal climate prediction and temporal memory. *Remote Sensing*, **15**(5), 1417.
- Yamada, H. (2020). Development of Maritime Education and Training Methods with Technological Innovation: Japan as a Case Study Focusing on MASS.
- Yu, H., Fang, Z., Murray, A. T. and Peng, G. (2019). A direction-constrained space-time prism-based approach for quantifying possible multi-ship collision risks. *IEEE Transactions on Intelligent Transportation Systems*, **22**(1), 131–141.
- Yu, H., Fang, Z., Fu, X., Liu, J. and Chen, J. (2021a). Literature review on emission control-based ship voyage optimization. *Transportation Research Part D: Transport and Environment*, **93**, 102768.
- Yu, H., Murray, A. T., Fang, Z., Liu, J., Peng, G., Solgi, M. and Zhang, W. (2021b). Ship path optimization that accounts for geographical traffic characteristics to increase maritime port safety. *IEEE Transactions on Intelligent Transportation Systems*, **23**(6), 5765–5776.
- Yu, H., Meng, Q., Fang, Z., Liu, J. and Xu, L. (2023). A review of ship collision risk assessment, hotspot detection and path planning for maritime traffic control in restricted waters. *The Journal of Navigation*, **75**(6), 1–27.
- Zăgan, R., Raicu, G., Hanzu-Pazara, R. and Enache, S. (2018). Realities in Maritime Domain Regarding Cyber Security Concept. In *Advanced Engineering Forum*, Vol. **27**. Trans Tech Publications Ltd, pp. 221–228.