Biographical Sketches

Unal Tatar, Ph.D.

Dr. Unal Tatar is an assistant professor at the Cybersecurity Department at the State University of New York at Albany. Dr. Tatar has been working on cyber risk management for over two decades as a professional and academic. He served as the head of Turkey's National Computer Emergency Response Team and an academic advisor at the NATO Center of Excellence Defense Against Terrorism on cyber threats. Dr. Tatar has three main lines of research: the economics of cybersecurity and risk management, critical infrastructure protection and national security, and cybersecurity capacity building. Dr. Tatar's research has been funded by federal and international organizations, including the National Science Foundation, the Department of Defense, the National Security Agency, the Air Force Research Laboratory, NATO, and the Society for Actuaries. Dr. Tatar holds a B.S. in Computer Science, an M.S. in Cryptography, and a Ph.D. in Engineering Management and Systems Engineering.

Bilge Karabacak, Ph.D.

Dr. Bilge Karabacak is an assistant professor at the Cameron School of Business at the University of North Carolina Wilmington. With 24 years of combined experience in academia, government, and industry, Dr. Karabacak brings a wealth of expertise to his academic research. Based on the limitations in existing risk analysis methods he observed during his tenure as an information security expert, he developed effective collaborative information security risk analysis methods, which are broadly cited and adopted. His research interests include information security risk analysis, cybersecurity maturity assessment, maritime cybersecurity assessment, critical infrastructure protection, IoT forensics, and decision-making in cybersecurity. He holds an M.S. in Computer Science and a Ph.D. in Information Systems with Cybersecurity specialization.

Omer F. Keskin, Ph.D.

Dr. Keskin is an Assistant Professor in the Cybersecurity Department at the College of Emergency Preparedness, Homeland Security, and Cybersecurity (CEHC) at the University at Albany, SUNY. He holds a Ph.D. in Systems Engineering and an M.S. in Digital Forensics and Cybersecurity. His research interests include organizational cyber risk management, cybersecurity of cyber-physical systems of critical infrastructure, computer network security, cyber insurance, and third-party risk management.

Dominick P. Foti

Dominick Foti is a Professional Lecturer of Computing Technology at Marist College. He is pursuing a PhD in Information Science with a concentration in Information Assurance. Dominick is also a Senior Researcher with the Cyber Deception & Behavior Science Laboratory at SUNY Albany, where he explores questions at the intersection of human behavior and cybersecurity. Dominick began his career developing cybersecurity intelligence for the Department of Homeland Security in 2014. Since then, Dominick has held roles with large corporations, such as Price Waterhouse Coopers and Advance Publications, consulting Fortune 500 companies on cybersecurity strategy, risk, vulnerability management, threat intelligence, application security, and incident response.

Title Page

Full Title: Charting New Waters with CRAMMTS: A Survey-Driven Cybersecurity Risk Analysis Method for Maritime Stakeholders

Authors and affiliations:

1st Author & Corresponding Author:

Name: Unal Tatar
Affiliation: University at Albany, State University of New York
Address: College of Emergency Preparedness, Homeland Security, and Cybersecurity
ETEC 260B, University at Albany, State University of New York
1400 Washington Ave., Albany, NY 12222 USA
E-mail: utatar@albany.edu

2nd Author:

Name: Bilge Karabacak
Affiliation: University of North Carolina Wilmington
Address: Congdon School of Supply Chain, Business Analytics and Information Systems
University of North Carolina Wilmington
Congdon Hall 2010, 601 S College Rd, Wilmington, NC 28403 USA
E-mail: karabacakb@uncw.edu

3rd Author:

Name: Omer F. Keskin
Affiliation: University at Albany, State University of New York
Address: College of Emergency Preparedness, Homeland Security, and Cybersecurity
ETEC 260G, University at Albany, State University of New York
1400 Washington Ave., Albany, NY 12222 USA
E-mail: okeskin@albany.edu

4th Author:

Name: Dominick P. Foti
Affiliation: Marist College
Address: School of Computer Science and Mathematics
John Winslow Dr, Poughkeepsie, NY 12601 USA
E-mail: dominick.foti@marist.edu

Charting New Waters with CRAMMTS: A Survey-Driven Cybersecurity Risk Analysis Method for Maritime Stakeholders

Unal Tatar
Department of Cybersecurity
University at Albany, SUNY
Albany, New York, USA
utatar@albany.edu

Bilge Karabacak
Congdon School of Supply Chain, Business Analytics and Information Systems
University of North Carolina Wilmington
Wilmington, North Carolina, USA
karabacakb@uncw.edu

Omer F. Keskin
Department of Cybersecurity
University at Albany, SUNY
Albany, New York, USA
okeskin@albany.edu

Dominick P. Foti
School of Computer Science and Mathematics
Marist College
Poughkeepsie, New York, USA
dominick.foti@marist.edu

Abstract

This article presents a novel survey-based cybersecurity risk assessment model, CRAMMTS (Cyber Risk Assessment Method for Maritime Transportation System), specifically designed for the maritime sector, addressing a critical gap in the literature. Our study contributes significantly in three ways: firstly, through a comprehensive critical literature review of 31 maritime guidelines and 95 scholarly articles, identifying the need for a new cybersecurity risk assessment method; secondly, by developing CRAMMTS, an adaptation of the ISRAM risk analysis method, incorporating the International Maritime Organization's criteria and enabling participation from maritime professionals, especially policymakers and leaders. The third contribution is a case study, the practical application of CRAMMTS in surveying 80 maritime professionals, assessing their perception of cybersecurity risks, and identifying varying risk levels, with the highest associated with cyber threat actors. This approach proved effective in assessing risks at both tactical and strategic levels and providing a clear, quantitative risk metric for decision-making. Our research underscores the maritime sector's need for a holistic, easily implementable cybersecurity risk analysis method that engages leaders and adapts to various Maritime Transportation System scopes, thereby enhancing cybersecurity risk assessment in this crucial domain.

Keywords: maritime cybersecurity, cyber risk assessment, information security risk, senior leadership engagement, survey-based methodology, ship cybersecurity, port cybersecurity

1 Introduction

The Maritime sector is an integral part of the world economy, ensuring the transportation of 1.5 billion short tons, equaling a value of $1.5 trillion, making shipping the primary mode of transportation for US trade in both weight and value. (Bureau of Transportation, 2020). Countries load and discharge approximately 21,279 million tons of goods (UNCTAD, 2021). It is no secret that disruption to this critical infrastructure sector, however brief, would have significant repercussions on the US economy and global markets.

Several recent events have provided insight into how disruptions to the Maritime sector can affect economic measures. The COVID-19 pandemic has had a prolonged effect on the shipping industry (Pijpker & McCombie, 2023). The initial effects of the outbreak caused a 3.8% drop in total volume in 2020 (UNCTAD, 2020). Millefiori et al. (2021) found that the mobility of ships was a vital issue resulting in this decreased volume, with the mobility of vessels dropping as much as 42.77% for passenger traffic and 13.77% for the shipping of goods. The Suez Canal incident is an example of how a local incident can severely impact global economic factors (Turner et al., 2024). In 2021, a sizable container ship crashed and lodged horizontally across the canal, resulting in around six days of impassibility (Reuters, 2021). About $15 – 17 billion of goods were estimated to be stopped because of the outage (Lee & Wong, 2021). Immediate inflation of prices was observed, with US gas prices increasing by $.40 in response to the obstruction (LeBlanc, 2021). These two incidents illustrate how shipping issues can have a massive impact on global trade.

While traditional disruptions to Maritime critical infrastructure are more significant than ever, cyber-attacks have been beginning to surface. A notable cyber attack on Maersk utilizing NotPetya ransomware caused around $200-300 million in losses, according to Maersk's 2017 Q2 Interim Report (A.P. Moller - Maersk, 2017). While infantile compared to previously mentioned disruptions, the potential adverse effects of cyber-attacks are astronomical.

Considering many of these recent maritime disruptions, the United States government has moved to enact the first maritime legislation in over 20 years. The US President designated cybersecurity of the Maritime Transportation Systems (MTS) as a top priority for national defense, homeland security, and economic competitiveness (White House, 2020). In 2022, President Biden signed the Ocean Reform Act in an effort to place the impact of delays on companies within the Maritime Sector instead of allowing these increased costs to trickle down the supply chain and eventually affect the prices of consumer goods and services. Rather than placing these fees on businesses and the consumer, shipping companies will be expected to take responsibility for these costs. While this bill was bipartisan and overtly supported, it sets a precedence of significant delays to be owned in major part by companies within the Maritime sector. Maritime organizations are now much more concerned about risks -including cyber risks- to the timeliness of their shipments, making risk assessment methodologies essential.

Risk assessment is a core component of the information security risk management process; therefore, it is vital for establishing and maintaining an information security management program. Despite these facts, managing cyber risks is one of the three challenges identified in the Great Disconnect Report (Chubb et al., 2022). According to the report, maritime leaders do not have a complete picture of technology risks and cyber threats. In the Safety at Sea and BIMCO Maritime Cyber Security survey performed in 2020, 77% of respondents viewed cyber-attacks as a high or medium risk to their organizations despite being unprepared in most cases (Mission Secure, 2021). An academic survey shows that 33% of the respondents encountered a cyber incident in the past year (Alcaide & Llave, 2020). Failing to recognize or assess the risks associated with maritime cybersecurity accurately can have tangible impacts on the stability and security of international trade and energy sectors (Loomis et al., 2021). Due to the potential impact of a significant cyberattack, organizations must be able to effectively measure the risk that cyber threats pose to maritime systems.

In this article, we proposed and applied a survey-based cybersecurity risk assessment model for the maritime sector by targeting the gap in the literature. This study has three major scientific contributions. First, we performed a comprehensive critical literature review focusing on identifying cybersecurity risk assessment methods proposed by researchers, governments, and NGOs for maritime and its assets. For this purpose, we critically reviewed 31 maritime guidelines and 95 scholarly articles. We shared the results of the critical literature review and described the gap in the literature that necessitates a new cyber risk assessment method for the maritime sector. Our second contribution is a survey-based cybersecurity risk analysis method that allows the participation of maritime professionals, particularly policymakers and leaders within the maritime sector. We named our model CRAMMTS: Cyber Risk Assessment Method for Maritime Transportation System. Notably, we customized the ISRAM risk analysis method for the maritime sector. We aligned IMO's impact and likelihood descriptions, risk categorization, risk mitigation options, and prioritizations with our proposed method. Our third contribution is applying the method by surveying 80 maritime professionals. We calculated five different risk values for different themes. Our goal was to assess the risk perceptions of maritime stakeholders, involving policymakers and top-level managers. Survey results showed that maritime stakeholders identified high and medium-level risks. Specifically, the risk analysis process involving questions regarding cyber threat actors produced a higher risk value than the risk analysis process involving questions regarding asset values. The lowest risk perception was for the asset-centric (sectoral and national security) theme. Our model provided risk results at both tactical and strategic levels. Our survey proved that this model enhances decision-making by providing an accurate, easy-to-comprehend, quantitative risk metric based on input from those charged with protecting maritime assets.

The organization of this paper is as follows. Following this introduction, the second section is dedicated to a comprehensive critical literature review. We described the gap in the literature in the third section. In the fourth section, we provided the details of CRAMMTS along with the details of the pilot risk assessment. The fifth section is dedicated to a discussion of the CRAMMTS method. The last section is the conclusion.

2 Literature Review

This section is dedicated to a comprehensive literature review that encompasses not only academic research but also grey literature, including studies, guidelines, and reports from governments, non-governmental organizations (NGOs), and other authoritative sources. We reviewed 31 guidelines and documents from international organizations, government agencies, NGOs, the private sector, and think tanks. We included six of them in our comparison tables within this section. We also reviewed 95 academic articles about maritime cybersecurity, mainly focusing on publications on cybersecurity assessments, vulnerability assessments, risk analysis, and risk management. We included 48 academic studies in which authors either developed a cyber risk analysis method for the maritime sector or performed cyber risk analysis.

This paper is a timely study as we developed and applied a risk analysis method after a comprehensive literature review and a clear view of the gap in the literature. After a systematic literature review and bibliometric analysis, Bolbot, Kulkarni, et al. identify 52 challenges and 73 future research topics in the maritime cybersecurity field (Bolbot, Kulkarni, et al., 2022). They showed that the top two hot research topics in maritime cybersecurity are developing or applying cybersecurity risk assessment techniques and designing monitoring and intrusion detection tools. Bolbot, Kulkarni, et al. identified nine challenges specific to the cybersecurity risk assessment process. The details of how we addressed some of these challenges are explained in Section 5.2 of this paper.

Drummond and Machado conducted a systematic literature review on cyber risk management of ports (Drummond & Machado, 2021). Only seven out of 93 publications addressed research questions regarding managing cyber risks of ports and provided a model or tool. Cyber risk management models include vulnerability assessment, attack path discovery, and incident reporting. However, the authors indicated that there is still a lack of a holistic model that provides a complete process for cyber risk management for ports. Our method promises a holistic risk assessment method for maritime transportation systems.

This literature review section comprises four parts: The first part provides pertinent information about maritime assets, vulnerabilities, and cyber incidents. The second part is dedicated to cybersecurity assessment guidelines developed by international organizations, governments, and NGOs; the third part shares the result of the critical literature review for academic papers, and the last part is the summary section for the literature review.

2.1 Maritime Assets, Vulnerabilities, and Cyber Incidents

It is essential to understand the different components of the maritime domain to understand the cybersecurity risks that apply to the Maritime sector. The Federal Maritime Commission defines its purview over what it defines as the "Ocean Supply Chain", which includes four regulated entities: Ocean Transportation Intermediaries (OTIs), Passenger Vessel Operators (PVOs), Vessel-Operating Common Carriers (VOOCs), and Marine Terminal Operators (MTOs). All these components heavily rely on information technology systems, and when evaluating cyber risks to the maritime sector, these entities should be considered in the scope of assessment. The maritime sector had been considered safe from cyber threats due to the lack of Internet connectivity and isolated Operational Technology (OT) environments. However, as the sector adopts digital technology, there has been an increase in cybersecurity breaches (Akpan et al., 2022).

Maritime Transportation Systems (MTS) consist of all the waterways, vessels, and ports used to move people and goods via water (Grobarcik et al., 2022). These systems are complex and enable the operational IT systems. For example, a commercial vessel may have at least 50 systems containing computing and software components (Chubb et al., 2022). The technological systems used in MTS can be categorized as Information Technologies (IT), Operational Technologies (OT), and communication systems (BIMCO et al., 2020; Meland et al., 2021). All of these systems create a global maritime cyberspace (White House, 2020).

Ship IT systems include administrative and passenger-related systems, while communication systems include satellites, very high-frequency (VHF) radios, and internal communications (Ashraf et al., 2022). OT systems are critical to maritime operations and consist of supervisory and physical level components such as sensors and actuators. These supervisory OT systems can be found on ships and include the Electronic Chart Display Information System (ECDIS), Automatic Identification System (AIS), integrated navigation systems, GPS, RADAR, alarm and distress systems, and Human-Machine Interaction (HMI) for other onboard OT systems. Other ship OT systems include engine, power, water, fuel, and cargo management systems for tracking, sensing, and temperature control (Ben Farah et al., 2022; BIMCO et al., 2020).

While many of these OT systems are utilized also in industries other than Maritime, ECDIS, and AIS and are unique to Maritime Technology Infrastructure and, thus, present unique risks (Akpan et al., 2022). For instance, AIS systems assist in communicating critical location-related information between shore and vessels. However, controls to ensure both the integrity and authentication of senders do not exist when data is in transit (Kessler, 2020, 2023). AIS architecture is unique and contains several sub-systems, such as time-division multiple access (TDMA), which provides a shared communication protocol between vessels; Digital Selective Call (DSC), which manages distress calls; Gaussian Minimum Shift Keying (GMSK), which provides modulation, and a Global Navigation Satellite System (GNSS) which assists with pinpointing vessel location. Researchers illustrated that fake AIS signals could be used to manipulate vessel location data. Attackers most likely did not propagate illegitimate "signals" but inserted data into publicly shared AIS databases, as AIS systems use unencrypted and unverified signals (Bergman, 2021; Harris, 2021). This introduces a significant risk to vessels, as decisions are made continuously during a voyage based on this information and during emergencies, such as search and rescue events. Decisions in such dire circumstances can be hindered if a malicious actor intercepts and manipulates this information.

Similarly, ECDIS, which provides critical data for vessel trajectory, has many vulnerabilities, both within the software and in the system's design (Ben Farah, 2022). In addition, Ben Farah et al. (2022) summarize common vulnerabilities of maritime-specific systems and other OT systems implemented within the Maritime industry. The analysis shows that spoofing, Denial of Service (DOS) attacks, and malware are pervasive across all Maritime OT systems. By evaluating these industry-specific systems, it is apparent that critical data, such as locational information, is at risk due to the OT where the data resides (Jacq et al., 2018).

The world has already experienced significant impacts from cyber incidents. Specifically, dozens of publicly reported cyber attacks have occurred within the maritime sector. While the impact of some incidents has been limited, some incidents, such as NotPetya, have reached costs up to hundreds of thousands of dollars. Due to the dependency of world trade on maritime transportation, the impact of incidents against maritime organizations has a ripple effect, causing negative impacts in other critical infrastructure sectors.

Attacks against the maritime sector can be categorized based on target types, such as IT attacks, OT attacks, and communication system attacks, regardless of where these systems are located. Attacks against IT networks do not require additional adversarial expertise compared to attacks on

IT networks of other critical infrastructure sectors; however, if networks are not properly segmented, adversaries can gain an initial foothold through attacks on IT and move laterally into OT systems. Attacks against the maritime sector can also be categorized by attack methods, such as ransomware, phishing, GPS spoofing, navigation system attacks, and malware. Ransomware and malware usually target IT systems, and phishing is utilized to gain initial access to organizational networks. On the other hand, GPS spoofing and navigation system attacks target OT systems (Meland et al., 2021).

In 2021, the IT systems of the Port of Houston were breached by government-backed hackers (Grobarcik et al., 2022). In June 2017, NotPetya Ransomware interrupted the operations of A.P. Moller-Maersk, a global shipping company that handles almost 20% of annual global freight. The incident led to an estimated cost of up to $300 million for Maersk (Mathews, 2017; Wienberg, 2017). Despite the significant costs, Maersk was not a specific target of a cyber-attack; instead, it was only one of the victim companies worldwide. Maersk's NotPetya ransomware incident shows how an IT-targeted attack can affect the operations of the maritime sector. Similar ransomware incidents victimized an additional five large shipping companies, COSCO, MSC, HMM, IRISL, and CMA CGM, as well as the Port of Hormuz (Crisis Group, 2023; Informa, 2020; Kapadia, 2020; Lopez, 2018; MSC, 2020; Roberts et al., 2019; Tabak, 2021; Torbati & Saul, 2012). Recently, operations at major ports in Australia were impacted by a cyberattack (Kovacks, 2023). The cyber-attacks caused 30,000 shipping containers to be stuck in port (Whitley & Doan, 2023). The attack impacted approximately 40% of freight into and out of Australia and crippled port activities (Liang, 2023). The trend of cyberattacks against MTS can be observed through the Maritime Cyber Attack Database (MCAD) (NHL Stenden, 2024). This database developed by researchers at NHL Stenden University of Applied Sciences in the Netherlands, tracks cyber incidents in the maritime sector. According to the data, the number of cyber incidents reported to MCAD has doubled every three years. The majority of recent incidents are ransomware and malware attacks.

The success of the OT attacks is primarily due to the lack of built-in security within these systems. Vulnerabilities that are common in industrial control systems are also observed in maritime OT systems, such as outdated or unused equipment connected to OT networks, poor network segmentation, insecure third-party connections, vulnerable wireless access points, outdated and unpatched operating systems and applications, and lack of encryption (Mission Secure, 2021). An example of an attack on OT systems occurred in 2013 when an oil rig in the Gulf of Mexico was shut down after a cyber incident. The oil rig had OT systems responsible for keeping the platform within a specific position using dynamic positioning and thrusters. These systems were on the same network as all other devices that the crew used. When users downloaded malware-infected music and video files from the internet, the malware infected the OT systems and caused a malfunction. Due to the incident, oil rig operations were halted (Harrington, 2013; Maritime Commons, 2015). Additionally, in May and June of 2017, three US military vessels were the victim of collisions due to attacks on their navigation systems (Ben Farah et al., 2022)

Nation-state adversaries pose the most risk to the maritime sector. The US National Maritime Cybersecurity Plan to the National Strategy details the activities and motivations of Iran, China, North Korea, and Russia against the maritime sector (White House, 2020). In February 2022, a maritime cyber security company discovered nation-state malware on seven vessels belonging to a large fleet. The malware was designed to provide attackers remote access with full privileges. This malware had been onboard the vessels for an estimated two years prior to the discovery (Chubb et al., 2022). Since maritime vessel networks were isolated, cybersecurity had not been a priority. In recent years, network connections between IT and OT networks have become widespread, whether on purpose or accidentally established. These connections increase the attack surface to the detriment of OT systems and allow malware to penetrate ship networks (Mission Secure, 2021).

2.2 Cybersecurity Risk Analysis and Management Guidelines

Risk analysis is an essential process to identify and prioritize risks; whereas risk management is the coordinated activities to direct and control an organization with regard to cybersecurity risks (ISO, 2018). Cybersecurity risk analysis is fundamental in identifying and prioritizing cybersecurity risks, irrespective of their source being technical or business process vulnerabilities (Baggott & Santos, 2020). While cybersecurity risk analysis and management guidance for most critical infrastructures have been maturing, it is noteworthy that authoritative bodies and NGOs in the maritime sector have substantially begun to provide such methodologies for the MTS since 2020. This section summarizes what governments, international organizations, and NGOs set forth about these essential topics.

The complex nature of maritime systems, characterized by the diversity of maritime assets and the multitude of threats they encounter, renders cybersecurity risk management in the maritime sector challenging and financially demanding. (Meland et al., 2021). The US executive branch published the National Maritime Cybersecurity Plan in December 2020 (White House, 2020). The plan emphasizes (1) the development of a threat-informed risk framework for port OT systems to enable self-assessments, (2) cybersecurity assessment of port facilities and vessels, and (3) Building on international frameworks such as the International Ship and Port Facility Security Code (ISPS Code) among other things related to risk analysis, information sharing, and workforce development. The ISPS code mandated by IMO identifies the minimum safety requirements for ships and ports that bind industry and government organizations.

Another mandate by IMO is the International Safety Management (ISM) Code. One of the goals of the ISM code is the safe management and operation of ships at sea. Two cyber risk management provisions were made to the ISM Code in 2016 and 2021, respectively. The 2021 circular, Guidelines on Maritime Cyber Risk Management, supersedes the 2016 resolution (IMO, 2021). The provisions serve as a trigger and essential milestone to start cybersecurity risk analysis and management processes within maritime companies and organizations. Guidelines on Maritime Cyber Risk Management mention an "urgent need" to raise cybersecurity awareness and provide five high-level recommendations of NIST’s Cybersecurity Framework (CSF) for managing cybersecurity risks: risk identification, asset protection, threat detection, incident response, and incident recovery. IMO’s Guidelines on Maritime Cyber Risk Management suggest maritime organizations three more additional guidance: (1) ISO/IEC 27001, (2) International Association of Classification Societies (IACS) Recommendation on Cyber Resilience (Rec 166), and (3)

Guidelines on Cyber Security Onboard Ships supported by 11 organizations (BIMCO et al., 2020; IACS, 2022; ISO, 2013).

NIST's CSF is referenced by IMO in its provision and served as a blueprint for the maritime risk analysis and management guidelines published by various organizations. Guidelines on Cyber Security Onboard Ships is the most comprehensive risk assessment and management guideline based on NIST's CSF. Cited in IMO's 2021 provision, the guidelines help maritime organizations develop cyber risk analysis and management processes in accordance with regulations and best practices, focusing on work processes, equipment, training, incident response, and recovery management (BIMCO et al., 2020).

UK's International Association of Classification Societies (IACS) released the Recommendation on Cyber Resilience in 2020 (IACS, 2022). It is the other cybersecurity guideline published by a maritime authority and cited in IMO's 2021 provision. The recommendation document is aligned with the five functions of NIST's CSF. The recommendation document provides detailed technical guidance to develop a program for cyber-resilient onboard OT systems and other systems connected to onboard OT systems. It does not describe a specific risk analysis method; instead, it provides basic requirements of risk assessment to be used in the program.

Digital Container Shipping Association (DCSA) published the Implementation Guide for Cybersecurity on Vessels in 2020 (DCSA, 2020). As the name implies, the guide elaborates on the Guidelines on Cyber Security Onboard Ships version 3 (A.K.A. BIMCO's guidelines) by dividing it into themes and mapping them into NIST CSF.

Cyber Security Workbook for On-Board Ship Use has been prepared as a practical guide to assist ship masters and officers in comprehending cybersecurity concepts in a straightforward manner. (BIMCO & International Chamber of Shipping, 2024). The document provides practical risk assessment guidance, such as the basic steps of risk management, key assessment questions and checklists, and sample risk assessment scripts for ECDIS & Shipboard Security System risk assessment. Cyber Security Workbook for On-Board Ship Use has been prepared as a practical guide; it does not suggest a model for cybersecurity risk assessment.

United States enacted the Maritime Transportation Security Act (MTSA) as a federal law in 2002. Entities in maritime transportation, including port facilities, vessels, and certain maritime-related businesses, should comply with MTSA. United States Coast Guard (USCG) published the Navigation and Vessel Inspection Circular (NVIC) 01-20 in 2020. The circular provides voluntary guidance for assessing and mitigating cyber vulnerabilities to comply with the MTSA. USCG has recently published the Maritime Cybersecurity Assessment and Annex Guide (MCAAG) in 2023. MCAAG does not supersede the NVIC 01-20; it supports it by providing more details on identifying cybersecurity vulnerabilities and selecting safeguards based on NIST CSF. US Coast Guard has also released the Vessel Cyber Risk Management Work Instruction for ISM Code compliance and Cyber Strategic Outlook, providing guidance and vision for the future of cyber risk in the maritime sector by identifying the roles, authorities, and key stakeholders and describing the lines of effort to secure maritime cyberspace.

Cyber Risk Management for Ports by ENISA introduces a four-phase approach to cyber risk analysis and management methods for port operators in the ecosystem (ENISA, 2020). The guideline does not provide a comprehensive methodology; instead, it shares actionable guidelines for cyber risk management that can be mapped to the frameworks that port operators use. After assessing cyber risks and security measures, the maritime organization can determine the cybersecurity maturity level of ports as basic, intermediate, or optimal. ENISA guidance suggests aligning cyber risks with physical security and safety through the ISPS Code. Cyber Risk Management for Ports is the only guidance document in this section that does not cite NIST CSF.

Table 1 summarizes the IMO's 2021 circular and five cybersecurity risk analysis and risk management guidelines for MTS. All guidelines provide detailed guidance on cybersecurity risk analysis; variations in the granularity of details are observed among different guidelines. Four guidelines are aligned with NIST CSF; this makes them a risk management guideline as well. Two guidelines were mentioned in IMO's 2021 circular. Only ENISA's guideline does not mention NIST's CSF and serves as a good practices document for cyber risk assessment that can be adapted to various risk assessment methodologies. Each of these guidelines, including the IMO circular, is voluntary, allowing organizations the discretion to adopt and implement them based on their individual needs and circumstances. All guidance documents target only some specific parts of the MTS, such as ships, port operators, and OT systems. Although IMO's Guidelines on Maritime Cyber Risk Management target all organizations in the shipping industry and all shipping operations, they do not detail a risk analysis process.

Table 1: Summary of risk management guidelines

The publication (Date)	**Prepared by**	**Targeted MTS**	**Mentions / Uses NIST CSF?**	**Goals & Focus**
Guidelines on Maritime Cyber Risk Management (June 2021)	International Maritime Organization	For all organizations in the shipping industry and all shipping operations	Yes	Serves as a call for action for risk management
The Guidelines on Cyber Security Onboard Ships version 4 (2020)	11 NGOs in the maritime sector	Ships	Yes	• Outlines and provides details of a risk analysis process • Assists in the development of a cyber risk management strategy

Recommendation on Cyber Resilience (April 2020)	International Association of Classification Societies (IACS), United Kingdom	Ships (OT systems and other systems that are connected to OT systems)	Yes	• Provides a roadmap for developing a program for cyber resilient computer-based systems on board, also serves as a framework for the security program • Provides basic requirements of a risk assessment process to be used in the program
Implementation Guide for Cybersecurity on Vessels (March 2020)	Digital Container Shipping Association (DCSA), The Netherlands	Ships operating in the container industry	Yes	• Provides the details of a quantitative risk analysis process • Provide a risk management framework that adheres to The Guidelines on Cyber Security Onboard Ships version 3
Maritime Cybersecurity Assessment and Annex Guide (MCAAG) (February 2023)	Coast Guard, United States	MTSA-regulated facilities	Yes	• Provides a process for identifying and describing cybersecurity vulnerabilities in the context of a Facility Safety Assessment • Provides implementation guidance for cybersecurity safeguards
Cyber Risk Management for Ports (December 2020)	ENISA, European Union	Port operators (both IT and OT systems)	No	• Shares good practices for risk analysis and risk management that can be mapped to the framework currently in use or to be used

As a result, six voluntary cybersecurity guidelines from government and NGOs have different goals and depths of details for risk analysis and risk management processes. Only three of the guidelines suggest a detailed risk analysis process. Among these three guidelines, *The Guidelines on Cyber Security Onboard Ships version 4* is the most comprehensive; it also provides a generic risk analysis method targeting ships and onboard systems. *Implementation Guide for Cybersecurity on Vessels* was prepared based on *The Guidelines on Cyber Security Onboard Ships version 3.* It provides templates for asset inventory and risk assessment processes. The guidelines are prepared for ships operating in the container industry. The third guideline that provides details of an assessment process is *the Maritime Cybersecurity Assessment and Annex Guide (MCAAG)*. It is less detailed than the other two guidelines; it provides guidance for identifying vulnerabilities within the context of Facility Safety Assessments.

2.3 Academic Studies on Maritime Cybersecurity Risk Analysis

Recent risk analysis and management recommendations from various maritime authorities and NGOs show the need for an easy-to-use and flexible cybersecurity risk analysis method for the maritime sector. Before starting an academic literature review, the main question was whether academia noticed the urgency of the matter and suggested cybersecurity risk analysis methods for maritime organizations. We confirmed that many researchers worldwide have been developing models and methods to assess the cyber security risks of maritime transportation systems.

In this section, we summarized 48 academic studies that propose a cybersecurity risk analysis method specific to the maritime sector or perform cybersecurity risk analysis for the existing maritime systems / using real maritime data. We included both risk analysis and risk management articles in our literature review. However, risk management as an organizational process has been defined by popular standards and guidelines such as NIST CSF, NIST Risk Management Framework (RMF), and ISO 27001. Therefore, academia extensively focuses on cybersecurity risk analysis, and risk management mainly falls outside the purview of most academic studies.

Svilicic et al. scanned the ECDIS on two vessels and discovered critical vulnerabilities. They used a popular commercial tool, Nessus, to perform vulnerability scans. The scanner discovered critical vulnerabilities in both ECDIS systems. ECDIS is an isolated system; therefore, the vulnerabilities do not have a direct impact. These studies contributed to developing maritime cybersecurity testing standard IEC 63154 (Svilicic, Rudan, Jugović, et al., 2019; Svilicic, Rudan, Frančić, et al., 2019). They did not perform a risk analysis; instead, they performed a vulnerability assessment. Vulnerability assessment results feed the risk analysis processes with actual data. In this regard, the studies provided essential contributions to the literature. Svilicic et al. also conducted a more comprehensive cyber risk assessment activity for a ship. Their approach consists of a survey conducted on a ship's crew and a vulnerability scan for the ship's ECDIS. They combined the findings of the survey and vulnerability scan and generated a risk matrix with likelihood and impact values for possible risk events (Svilicic, Kamahara, et al., 2019).

Patterson and Bridgelall performed a risk analysis for the San Diego port. They utilized the Threat, Vulnerability, and Consequence (TVC) model of the Risk Analysis and Management for Critical Asset Protection (RAMCAP) framework used by the Department of Homeland Security (Patterson & Bridgelall, 2020). In the TVC model, the risk is the multiplication of Threat, Vulnerability, and Consequence parameters. The study showed that risk is higher for cruise ships than container ships. Even for cruise ships, the risk level is below the threshold because of low vulnerability levels. The authors suggested improving security culture with the help of policies to minimize negligence and ignorance.

Gunes et al. proposed a 13-step quantitative cybersecurity risk analysis (Gunes et al., 2021). They shared the details of their model, including risk formulas and reference tables for vulnerability rating, likelihood, and impact values. They applied their risk analysis model on a port facility for four different cyber security attack scenarios. For each scenario, they identified high-level risks that require risk mitigation efforts. They shared the risk analysis results with IT staff to raise awareness.

Tam and Jones proposed the Maritime Cyber-Risk Assessment (MaCRA), which provides a risk assessment model based on the unique characteristics of the maritime industry (Tam & Jones, 2019). MaCRA has an open quantitative model based on ease-of-exploit, the reward of the attack, and vulnerability level parameters. MaCRA can be applied to any combination of ship, system, environment, and attacker. They did not share any application results and findings of the model in their publication. Tam and Jones applied MaCRA for autonomous ships as well (Tam & Jones, 2018). Researchers specifically look at near-future ships currently in prototype form.

Bolbot et al. employed a Cyber Preliminary Hazard Analysis (CPHA) for an autonomous ship's navigation and propulsion control system (Bolbot et al., 2019, 2020). They included IMO's Formal Safety Assessment (FSA) risk matrix in ranking the hazardous scenarios. They discovered technical vulnerabilities in several communication and OT systems. They suggested adding firewalls, intrusion detection systems, and redundant lines to mitigate the risk. Bolbot, Basnet, et al. diverted to a cyber risk analysis method that adapts and integrates five existing methods, which are STRIDE, ATT&CK, SysML, System-Theoretic Process Analysis (STPA), and ranking methods, to more effectively assess the cyber risks posed by the remote pilotage of ships (Bolbot, Basnet, et al., 2022). They implemented SysML to visualize components and activities of remote pilotage systems, STPA to analyze hazards, and STRIDE and ATT&CK to analyze various attack vectors. The findings of the analysis indicate that the most critical threats to remote pilotage systems are denial of service, spoofing, and tampering. Bolbot et al. then took the initial CPHA conducted in 2019 and 2020 and built on this work by proposing a novel Hazard Identification (HAZID) risk assessment methodology for autonomous inland waterways ships (Bolbot et al., 2023). The proposed assessment is a semi-structured expert-based process that specifically targets the design phase of these ships and looks at safety, cybersecurity, and security threats as part of the scope of the assessment. Existing regulatory risk assessment processes, such as the FSA risk matrix, were used to support this methodology.

Park et al. introduced a novel risk assessment framework for six categories of maritime cyber threats, merging Failure Mode and Effects Analysis (FMEA) with a Rule-based Bayesian Network (RBN) (Park et al., 2023). After evaluating six threat categories, researchers identified malware as the most critical risk, followed by phishing and human factors, after conducting two questionnaires. They validated the threats identified from the literature in the first questionnaire through the participation of maritime experts before starting the second questionnaire with 100 maritime industry experts. The proposed FMEA-RBN methodology offers advantages in handling uncertainties in maritime cybersecurity, incorporating both objective and subjective data.

Iphar et al. addressed emerging cyber threats in maritime navigation, proposing a risk assessment method focusing on the Automatic Identification System (AIS) (Iphar et al., 2020). More specifically, they propose a method for the integrity assessment of AIS messages and the consequent risk analysis using real data for four experimental cases. Six individuals, spanning civil and military sectors, collaborated in various stages, contributing to risk analysis of the AIS, defining maritime situations, setting data thresholds, and providing guidance for efficient risk display.

Amro et al. proposed a risk management framework for autonomous passenger ships. They assessed the dependencies among the components of autonomous vessels and evaluated the impact of the security and safety countermeasures (Amro et al., 2020). The framework proposed feeds the findings of Preliminary Hazard Analysis and STRIDE into the Six-Step Model. The framework suggested an approach to improve the safety and security of a system under development. Among others, implementing secure network protocols and having proper security monitoring measures and incident response plans are identified as the most effective countermeasures for security and, indirectly, for the safety of autonomous passenger ships. Amro and Gkioulos used a novel approach of defense-in-depth and threat-informed defense to manage risk for autonomous passenger ships, such as ferries (Amro & Gkioulos, 2023a). The authors used a real autonomous ship system called milliAmpere2 as a use case for their proposed methodology. Data from the Mitre Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework was used to contextualize threats. Amro and Gkioulos also proposed an evaluation methodology for cyber-physical system risk assessment methodologies (Amro & Gkioulos, 2023b). To demonstrate the evaluation methodology, they conducted two different risk assessment processes on two different use cases; one of the use cases was an autonomous passenger ship. The results include insights regarding applicability, feasibility, accuracy, scalability, and usability. A recently developed cyber risk methodology by the authors, which combines Failure Modes Effects and Criticality Analysis with ATT&CK, was analyzed using the evaluation methodology to validate its success by several experts from the maritime and cybersecurity domains.

Andrews et al. proposed a risk assessment approach for waterways (Andrews et al., 2020). They adapted corridor trace analysis, which was initially developed as a risk assessment method for roads on land. The model divides the inland waterway into segments and assesses the risks based on several factors, including channel geometry, obstacles, environment, and threats that might include cyber threats. Outputs of the analysis include visualization of the segments for operational safety and security decision-making.

Chang et al. conducted a risk assessment for autonomous ships with an approach that combines Failure Modes and Effects Analysis (FMEA), Evidential Reasoning, and a Rule-based Bayesian Network to rank hazardous events (Chang et al., 2021). Their results indicate that the top three hazards are interacting with crewed vessels and objects, cyber-attacks, and human error in designing autonomous vessel software.

Jacq et al. developed a hybrid testbed with a mix of real and virtualized OT and IT systems where cyber attack scenarios on ports can be simulated and analyzed (Jacq et al., 2021). Furthermore, the outputs of the scenario are used by a proposed cyber risks assessment methodology to simulate the impact of the disruption on the macroeconomic level. The testbed can be used for the tactical-level analysis of cyber risks that can be further used for strategic-level analyses.

Bernsmed et al. proposed utilizing bow-tie diagrams for cyber security risks in addition to their traditional use on safety risk analysis (Bernsmed et al., 2018). The combined safety and security analysis proposed can be used by organizations in the maritime domain for analyzing the causes, likelihood, and impact of cyber incidents and visualizing the findings for prioritization. They discussed that adding threat actors and vulnerabilities to this method would be possible despite presenting unnecessary complexity.

Paul et al. developed and applied a collaborative cyber risk management approach to maritime cyber risks (Paul et al., 2021). Using the tool that employs the EBIOS Risk Manager method, various cyber risk scenarios for ship systems were analyzed by deriving insights from the asset owners and cybersecurity experts.

Schauer et al. proposed a risk management methodology for cyber risks in the maritime domain (Schauer et al., 2019). The methodology includes analysis from individual assets to the supply chain level. The qualitative model starts with analyzing all the software on each hardware connected to the network by listing their known vulnerabilities. It continues the analysis by considering the interdependency relationships among assets within an organization and among different organizations within the supply chain. The methodology then allows for conducting game-theoretic analysis of various mitigation strategies against attack scenarios. One limitation of the supply chain level analysis is that it requires collaboration from all entities of the supply chain, which could lead to privacy and data sharing concerns.

Yoo and Park conducted a qualitative risk assessment to identify cyber risk components for administrative, technical, and physical security risk components (Yoo & Park, 2021). They further analyzed the survey findings using the Analytical Hierarchy Process to prioritize cyber risk components. Their findings indicate that the most important mitigation activities are increasing awareness of cyber risks, implementing access control, and improving detection and response capabilities.

Niemiec et al. proposed a risk management framework considering the dependency relationships among different sectors (Niemiec et al., 2022). It provides a strategic-level analysis of cyber risks. They analyzed existing frameworks and concluded that they cannot address trans-sectoral and transversal issues. The proposed framework has analyzed the challenges and opportunities of cybersecurity considering technological, transversal, and inter-sectoral aspects.

Farah et al. conducted a high-level risk assessment for various tactical-level maritime scenarios using a basic qualitative risk assessment approach and provided mitigation strategies for various risk events (Farah et al., 2023). The scenarios include cyberattacks on a tugboat, docking and maneuvering systems of a ship, and berthing aid systems. The scenarios were analyzed from various perspectives, and mitigation strategies were provided.

Li et al. researched the safety of Maritime Autonomous Surface Ships (MASS) by identifying operational risks and analyzing their causal relationships using network modeling (Li et al., 2023). They contributed to an integrative approach to operational risk analysis, offering insights into potential risks and managerial implications for risk control in MASS operations.

Melnyk, Onyshchenko, Onishchenko, et al. proposed a risk assessment technique to calculate the risk and monetary impact of cyber incidents (Melnyk, Onyshchenko, Onishchenko, et al., 2022). The method calculates the risk for each type of system of a ship by also considering the magnitude of the threats, the level of vulnerability, and the value of the system and cargo.

Melnyk, Onyshchenko, Pavlova, et al. proposed a mathematical programming task to assess the cyber risks of ships, although they did not apply the model (Melnyk, Onyshchenko, Pavlova, et al., 2022). The proposed approach aimed to suggest reliable and economically feasible mitigation from the identified risks. The authors indicated that there is no single approved approach for cyber risk assessment and the risk landscape would vary for different companies.

Nguyen et al. conducted a risk assessment for blockchain-integrated systems of the maritime logistics sector (Nguyen et al., 2022). The mixed-method risk analysis included interviews and surveys and provided a set of failure modes of blockchain applications, including data breaches and ransomware.

Progoulakis et al. applied the bow-tie analysis method to analyze the cyber risks of maritime transportation and port infrastructure (Progoulakis et al., 2023). The qualitative analysis identified the three most significant threats: malicious remote network access, malware infection through the internet, and cloud server data breach. The authors suggested improvements in vulnerability management and employing other cyber risk assessment methods that have proven to work in other industries.

Rajaram et al. conducted a qualitative cyber risk assessment on onboard ship Operational Technology (OT) systems (Rajaram et al., 2022). The authors developed cyber risk assessment and mitigation guidelines to provide a practical resource for shipowners and authorities.

Yungratog et al. proposed a conceptual framework for risk assessment for protected data handled by maritime sector IT networks (Yungratog et al., 2022). The framework leverages the existing Data Protection Impact Assessment method to apply to the maritime domain.

Pavlinovic et al. instituted a survey-based approach to understand the level of knowledge of cyber threats among Croatian maritime sector members (Pavlinovic et al., 2022). This research found that while those within the sample understood the risks of cybersecurity threats, lack of awareness and education within the maritime sector and cost are major barriers to defending against cyber threats.

De Peralta et al. developed a 2-part manuscript that addressed risk management within Maritime Renewable systems; the first part addressed the identification of vulnerabilities and determining of risk, while the second addressed solutions to vulnerabilities and risks identified in the first (De Peralta et al., 2020, 2021). Risks were identified through stakeholders and publicly available sources in conjunction with NIST Frameworks, such as the NIST Cyber Security Framework. Then, a framework for risk management was provided by combining guidance from NIST and maritime industry standards.

Hemminghaus et al. initialized an offensive tool specifically designed to test the security of maritime systems(Hemminghaus et al., 2021). The attacks within the tool's scope include spoofing, eavesdropping, replaying, injection, and obfuscating network traffic between maritime-specific IT/OT systems. This tool can be used to assist in the verification of vulnerabilities in the risk assessment process for maritime systems.

Kalogeraki et al. proposed a risk assessment methodology called MITIGATE, specifically for cyber-physical and SCADA systems within Maritime and Logistics infrastructure (Kalogeraki et al., 2018). This methodology assists maritime organizations in achieving ten objectives related to the risk management lifecycle, from asset risk evaluation to formulating risk mitigation strategies.

These ten objectives can be operationalized through eight security assessment services, including but not limited to vulnerability management, threat management, and supply chain risk analysis. Although this risk assessment methodology applies to the maritime industry, many aspects focus on supply chain management.

Kavallieratos et al. proposed a more general risk management framework for cyber-physical systems, allowing for the efficient selection of cybersecurity controls by aggregating individual risk assessments of components (Kavallieratos et al., 2021). In addition, an automated mechanism is proposed to select controls based on residual risk and implementation cost minimization. The authors applied this cyber risk framework to the maritime industry, specifically autonomous and remote-controlled ships.

Kuhn et al. evaluated the risk of cyber attacks on maritime systems through the lens of the COVID-19 Pandemic, including paradigm shifts in how experts view risk due to the pandemic (Kuhn et al., 2021). Scenarios were presented to experts from a NATO Centre of Excellence Defence against Terrorism (COE-DAT) to understand how a group perceives risk in the context of the maritime industry. It was found that group settings lent themselves to identifying a better risk measurement, with government/public officials having different strengths and weaknesses when responding to incidents.

Polatidis et al. used attack graph analysis methods, including constraints and depth-first search, to discover new attack paths for maritime ports (Polatidis et al., 2018). Due to the use of real data from the Port of Valencia, the development of privacy and data quality techniques was also completed.

Tusher et al. used a multi-criteria decision-making methodology to evaluate risk within the maritime industry (Tusher et al., 2022). Surveying was used to evaluate and rank maritime systems by susceptibility to cyberattacks using the knowledge of subject matter experts. It was found that navigational systems were most susceptible to cyber-attacks, while propulsion systems were least susceptible. Experts were also surveyed for possible approaches to risk mitigation strategies.

Kayisoglu et al. use the SLIM-based human reliability analysis method to calculate the probability of human error for ECDIS (Kayisoglu et al., 2022). This risk analysis can be used to understand the human risk within maritime systems better, influencing policy mitigation approaches.

Kechagias et al. present a case study of a maritime organization's strategic implementation of cybersecurity strategy (Kechagias et al., 2022). Cyber risks were addressed through multiple approaches (i.e., mitigation, acceptance, transference) and were identified through survey questions. The overall attitudes towards cyber threats were also collected.

Lampreia et al. implemented risk matrices for autonomous software in both ships and at ports (Lampreia et al., 2022). The authors applied this methodology to a Portuguese Naval ship's maintenance system. Specifically, risk to the data within the database supporting the maintenance system was assessed.

Pöyhönen et al. conducted a cybersecurity risk assessment on the data in transit between ships and cloud systems (Pöyhönen, 2022). This paper applied a methodology developed in a previous paper by Pöyhönen and Lehto, which uses attack graphs to measure both threat vectors and defensive opportunities according to The NIST Cybersecurity Framework (Pöyhönen & Lehto, 2022). Pöyhönen et al. applied this risk assessment in the additional use case of smart terminals (Pöyhönen, 2023).

Söner et al. used failure modes and effects analysis to understand which cybersecurity-related vulnerabilities and associated attacks are applicable to voyage data recorder systems (Söner et al., 2023). Both specific attacks and especially vulnerable components are identified, and associated controls are established.

2.4 Summary of Risk Analysis Methods

This section provides a detailed overview of the various risk assessment models for Maritime Transportation Systems (MTS), as illustrated in Table 2. The table encapsulates a comprehensive summary of guidelines and academic research focusing on risk assessment models pertinent to MTS. It specifically outlines the scope of risk analysis, the analysis's level, and whether the assessment was conducted on an existing system or utilized real-world data.

In the context of our paper, if a risk assessment method or application targets the tactical level, they identify operational-level risks, such as risks at computer systems and day-to-day tactical operations. Strategic-level risk analysis focuses on identifying risks at both the sector-wide and national levels, as well as assessing risks within the business processes of an organization.

The first three rows of Table 2 are reserved for three guidelines, whereas the remaining rows are dedicated to 48 risk analysis methods proposed in scholarly studies.

Table 2: Summary of guidelines and risk analysis papers

Guideline / Academic study	**The scope of the analysis**	**The level of the analysis (Tactical / Strategic)**	**Was the analysis performed on existing systems?**	**Was the analysis performed using real data?**
The Guidelines on Cyber Security Onboard Ships version 4	Ships	Tactical	N/A	N/A
Implementation Guide for Cybersecurity on Vessels	Vessels operating in the container industry	Tactical	N/A	N/A
The Maritime Cybersecurity Assessment and Annex Guide (MCAAG)	MTSA-regulated facilities	Tactical	N/A	N/A

Guideline / Academic study	The scope of the analysis	The level of the analysis (Tactical / Strategic)	Was the analysis performed on existing systems?	Was the analysis performed using real data?
(Svilicic, Rudan, Jugović, et al., 2019; Svilicic, Rudan, Frančić, et al., 2019)	ECDIS	Tactical	Yes	No
(Svilicic, Kamahara, et al., 2019)	Ship	Tactical	Yes	Yes
(Patterson & Bridgelall, 2020)	Port	Tactical	Yes	Yes
(Gunes et al., 2021)	Port	Tactical	Yes	No
(Tam & Jones, 2018)	Autonomous Ships,	Tactical	No	No
(Tam & Jones, 2019)	Any combination of ship, system, environment, and attacker	Tactical	No	No
(Bolbot et al., 2019, 2020)	Navigation and propulsion systems of an inland autonomous ship	Tactical	Yes	No
(Park et al., 2023)	Maritime sector	Tactical	No	No
(Iphar et al., 2020)	AIS	Tactical	No	Yes
(Amro et al., 2020)	Autonomous Passenger Ship	Tactical	Yes	Yes
(Andrews et al., 2020)	Waterway/canal operational risk assessment	Tactical	Yes	Yes
(Chang et al., 2021)	Autonomous surface ships	Tactical	Yes	Yes
(Jacq et al., 2021)	Port	Tactical	No	No
(Bernsmed et al., 2018)	Any cyber risk event in the maritime domain	Tactical	No	No
(Paul et al., 2021)	Ship	Tactical	No	No
(Schauer et al., 2019)	Maritime supply chain	All	Yes	No
(Yoo & Park, 2021)	Ship	Tactical	No	Yes
(Amro & Gkioulos, 2023b)	Autonomous Passenger Ship	Tactical	Yes	Yes
(Bolbot, Basnet, et al., 2022)	Remote pilotage of ships	Tactical	Yes	Yes
(Niemiec et al., 2022)	Maritime Domain	Strategic	No	No
(Farah et al., 2023)	Ship and Port	Tactical	Yes	Yes

Guideline / Academic study	The scope of the analysis	The level of the analysis (Tactical / Strategic)	Was the analysis performed on existing systems?	Was the analysis performed using real data?
(Li et al., 2023)	Surface autonomous ship	Tactical	Yes	No
(Melnyk, Onyshchenko, Onishchenko, et al., 2022)	Ship	Tactical	No	No
(Melnyk, Onyshchenko, Pavlova, et al., 2022)	Ship	Tactical	No	No
(Nguyen et al., 2022)	Blockchain-integrated systems of maritime logistics	Tactical	Yes	Yes
(Progoulakis et al., 2023)	Maritime infrastructure in general	Strategic	No	No
(Rajaram et al., 2022)	Ship	Tactical	No	No
(Yungratog et al., 2022)	Systems that handle Personal Data (under the scope of GDPR)	Tactical	No	No
(Pavlinovic et al., 2022)	Croatian Maritime Sector	Strategic	Yes	No
(Bolbot et al., 2023)	Autonomous inland ships	Tactical	Yes	Yes
(De Peralta et al., 2020, 2021)	Marine Renewable Energy Systems	Tactical	No	No
(Hemminghaus et al., 2021)	Ship	Tactical	Mixed	Mixed
(Kalogeraki et al., 2018)	Maritime Supply Chain	Tactical	Mixed	Mixed
(Kavallieratos et al., 2021)	Autonomous and Remote-controlled Ships	Tactical	Yes	No
(Kuhn et al., 2021)	Maritime Domain	Strategic	No	No
(Polatidis et al., 2018)	Ports	Tactical	Yes	Yes
(Tusher et al., 2022)	Autonomous Ships	Strategic	Yes	No
(Amro & Gkioulos, 2023a)	Autonomous Passenger Ships	Tactical	Yes	Yes
(Kayisoglu et al., 2022)	ECDIS	Tactical	Yes	Yes
(Kechagias et al., 2022)	Maritime Domain	Tactical	Yes	Yes
(Lampreia et al., 2022)	Automation Software (Port and Ship)	Tactical	Yes	Yes

Guideline / Academic study	The scope of the analysis	The level of the analysis (Tactical / Strategic)	Was the analysis performed on existing systems?	Was the analysis performed using real data?
(Pöyhönen, 2022)	Ship-to-Cloud Information Flows	Tactical	Yes	No
(Pöyhönen, 2023)	Smart Terminals	Tactical	Yes	No
(Pöyhönen & Lehto, 2022)	Maritime Domain	Tactical	Yes	No
(Söner et al., 2023)	VDR	Tactical	Yes	No

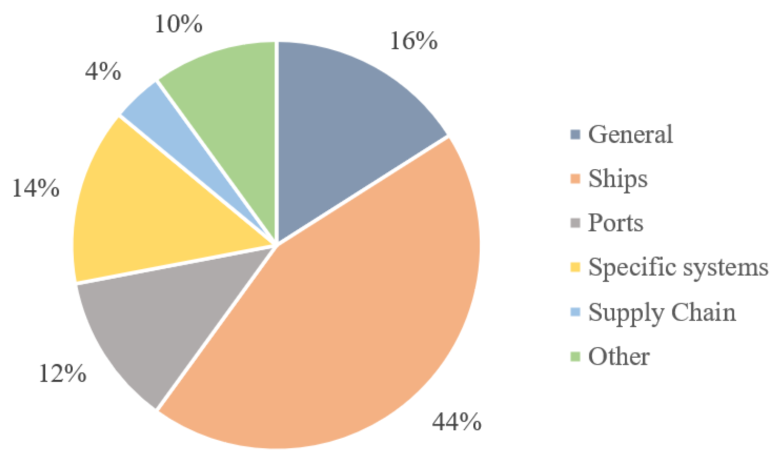

Figure 1: Scope of Analysis for Risk Analysis Papers

Evaluating the statistics of each type of data collected for each manuscript highlights interesting themes. First, ships were the primary scope of analysis for manuscripts, as shown in Figure 1. The main sub-scope was autonomous ships, which comprised 50% of the researchers conducting risk assessments or creating risk models for ships. Researchers secondarily focused on the maritime industry as a whole, followed by specific systems (i.e., VDA, ECDIS), ports, and finally, other systems, such as blockchain maritime systems and privacy-related systems.

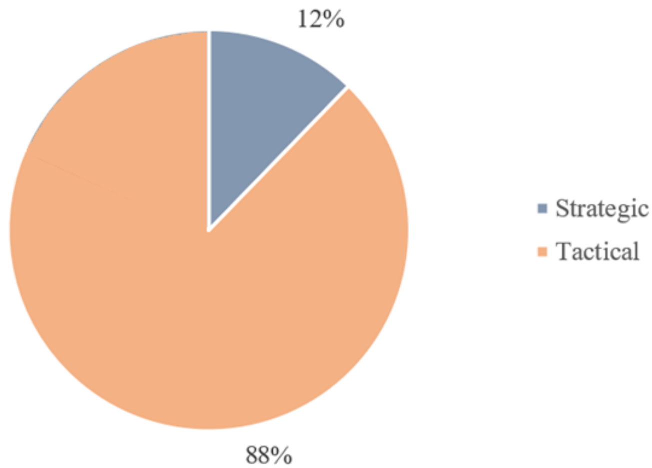

Figure 2: Level of Analysis for Risk Analysis Papers

The level of analysis is summarized in Figure 2. Most papers focused on a tactical level of analysis; it was found that papers seldom offered a strategic level analysis approach. One manuscript (Schauer et al., 2019) provided a model that assessed all levels of analysis.

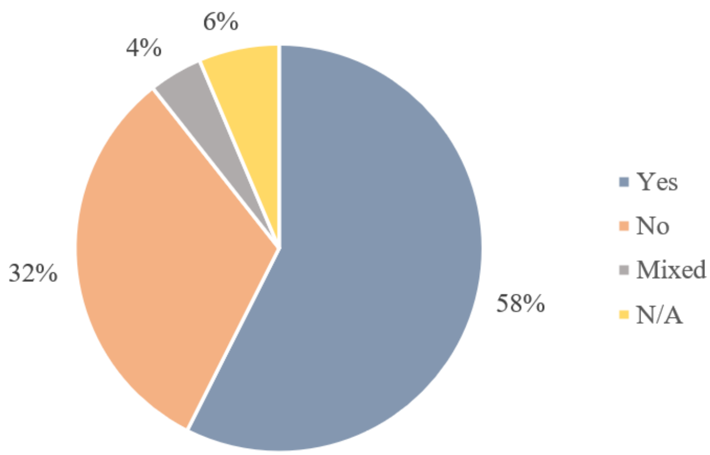

Figure 3: Distribution of papers according to their application to existing systems

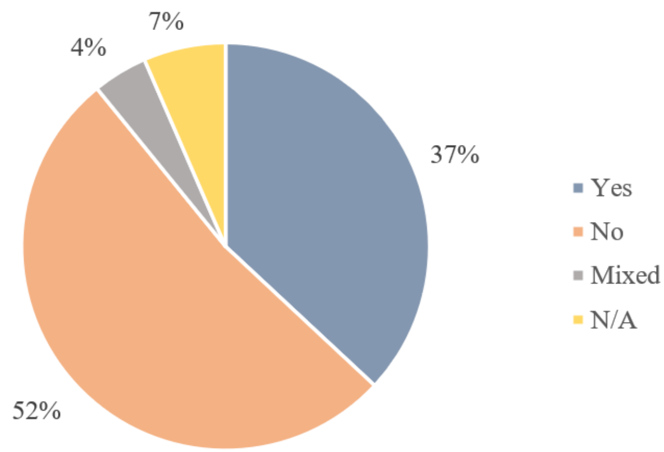

Figure 4: Distribution of papers according to their application on real data

The final two elements of data gathered pertained to whether the studies examined existing systems, as depicted in Figure 3, and if they incorporated real data into their analysis, which is illustrated in Figure 4.While authors were predominately able to conduct analysis on existing systems, a smaller portion of papers were able to use real data in their analysis. It was found that only 15 papers were able to utilize both existing systems and real data within their analysis.

3 Gap in the Literature

To better understand the gap in the literature, we identified three requirements for an ideal maritime cybersecurity risk analysis method by performing semi-structured interviews with three cybersecurity experts with a reputable research record on critical infrastructure security and two IT professionals with two decades of experience working in the maritime sector. Three requirements are:

1) Implementability
2) Leadership engagement
3) Adaptability

The motivation behind the implementability and leadership engagement is that the number of IT and cybersecurity experts in the maritime sector is quite limited compared to the other critical sectors. Moreover, maritime leaders lack a complete picture of the technology risks and cyber threats. A risk analysis method that is easy to implement and allows the participation of leaders would improve the security posture of the organization. Adaptability is just another point stressed by maritime cybersecurity and IT experts. There could be different scopes and scenarios for maritime cybersecurity risk analysis, and a method that can easily be customized to different scopes and circumstances could be beneficial for maritime organizations. It also involves the ease of integration into existing risk management frameworks such as ISO 27001, NIST CSF, and NIST RMF.

We determined three levels for each requirement: Easy, Moderate, and Challenging. Table 3 provides the descriptions of these levels for each requirement.

Table 3: Descriptions of three levels for requirements

Requirement	Easy	Moderate	Challenging
Implementability	The method can be easily implemented by a maritime organization.	The method can be implemented by the involvement of a third-party contractor.	The method describes a theoretical framework. It can only be applied by academics.
Leadership engagement	The method allows the participation of maritime leaders and policymakers.	The method can only allow the participation of mid-level / tactical managers.	The method does not allow the participation of maritime leaders, or the method is not designed to include maritime personnel.
Adaptability	The method can easily be customized for different scenarios and scopes; the method can easily be integrated into the existing risk management framework adopted by the organization.	Third-party involvement is required to customize the method for different scenarios and scopes, or the customization is possible but challenging; integrating the method into the existing risk management framework adopted by the organization is possible but not straightforward.	The method cannot be customized for different scenarios and scopes; it is a challenging task to integrate the method into the existing risk management framework adopted by the organization.

Table 4 evaluates the risk analysis methods in three guidelines and 48 academic papers based on the levels described in Table 3.

Table 4: Evaluation of risk analysis methods proposed in guidelines and academic papers

Guideline / Academic study	Implementability	Leadership engagement	Adaptability
The Guidelines on Cyber Security Onboard Ships version 4	Moderate	Challenging	Easy
Implementation Guide for Cybersecurity on Vessels	Easy	Moderate	Easy
The Maritime Cybersecurity Assessment and Annex Guide (MCAAG)	Moderate	Challenging	Easy
(Svilicic, Rudan, Jugović, et al., 2019; Svilicic, Rudan, Frančić, et al., 2019)	Easy	Challenging	Moderate
(Svilicic, Kamahara, et al., 2019)	Easy	Moderate	Moderate
(Patterson & Bridgelall, 2020)	Easy	Challenging	Moderate

Guideline / Academic study	Implementability	Leadership engagement	Adaptability
(Gunes et al., 2021)	Moderate	Easy	Easy
(Tam & Jones, 2018)	Challenging	Moderate	Easy
(Tam & Jones, 2019)	Challenging	Moderate	Easy
(Bolbot et al., 2019, 2020)	Moderate	Challenging	Challenging
(Park et al., 2023)	Moderate	Challenging	Moderate
(Iphar et al., 2020)	Challenging	Challenging	Challenging
(Amro et al., 2020)	Challenging	Challenging	Moderate
(Andrews et al., 2020)	Moderate	Challenging	Moderate
(Chang et al., 2021)	Challenging	Easy	Moderate
(Jacq et al., 2021)	Moderate	Easy	Moderate
(Bernsmed et al., 2018)	Moderate	Moderate	Easy
(Paul et al., 2021)	Easy	Easy	Moderate
(Schauer et al., 2019)	Challenging	Moderate	Moderate
(Yoo & Park, 2021)	Moderate	Moderate	Moderate
(Amro & Gkioulos, 2023b)	Challenging	Easy	Challenging
(Bolbot, Basnet, et al., 2022)	Challenging	Challenging	Moderate
(Niemiec et al., 2022)	Moderate	Easy	Moderate
(Farah et al., 2023)	Easy	Challenging	Easy
(Li et al., 2023)	Challenging	Challenging	Moderate
(Melnyk, Onyshchenko, Onishchenko, et al., 2022)	Easy	Moderate	Moderate
(Melnyk, Onyshchenko, Pavlova, et al., 2022)	Easy	Challenging	Moderate
(Nguyen et al., 2022)	Challenging	Challenging	Challenging
(Progoulakis et al., 2023)	Easy	Moderate	Moderate
(Rajaram et al., 2022)	Moderate	Moderate	Moderate
(Yungratog et al., 2022)	Challenging	Challenging	Challenging
(Pavlinovic et al., 2022)	Challenging	Easy	Easy
(Bolbot et al., 2023)	Moderate	Moderate	Moderate
(De Peralta et al., 2020, 2021)	Moderate	Moderate	Easy
(Hemminghaus et al., 2021)	Moderate	Challenging	Moderate
(Kalogeraki et al., 2018)	Moderate	Moderate	Easy
(Kavallieratos et al., 2021)	Challenging	Moderate	Easy
(Kuhn et al., 2021)	Moderate	Easy	Moderate
(Polatidis et al., 2018)	Challenging	Challenging	Challenging
(Tusher et al., 2022)	Challenging	Easy	Challenging
(Amro & Gkioulos, 2023a)	Moderate	Challenging	Moderate
(Kayisoglu et al., 2022)	Challenging	Moderate	Challenging
(Kechagias et al., 2022)	Easy	Moderate	Moderate
(Lampreia et al., 2022)	Moderate	Challenging	Challenging
(Pöyhönen, 2022)	Moderate	Moderate	Moderate
(Pöyhönen, 2023)	Moderate	Moderate	Moderate
(Pöyhönen & Lehto, 2022)	Moderate	Moderate	Moderate
(Söner et al., 2023)	Challenging	Challenging	Moderate

Three risk analysis guidance documents listed in Table 4 share some common properties. They fit well into an existing risk management framework as they all use the approach suggested by NIST CSF. They are all paper-based methods. They do not require the use of complex calculations and mathematical tools. *The Guidelines on Cyber Security Onboard Ships version 4* and *Implementation Guide for Cybersecurity on Vessels* provide details on threats and vulnerability identification and likelihood and impact assessments in addition to risk assessment. *Implementation Guide for Cybersecurity on Vessels. Maritime Cybersecurity Assessment and Annex Guide (MCAAG)* focuses only on vulnerability identification and assessment.

The Guidelines on Cyber Security Onboard Ships version 4 emphasizes the importance of senior management involvement in the risk analysis process by reminding that cyber risks could affect business processes and will require the allocation of resources for mitigation efforts, among other things. The risk analysis team should find ways to involve the senior leadership in the risk analysis processes described in the Guidelines on Cyber Security Onboard Ships version 4. The same fact applies to *the Implementation Guide for Cybersecurity on Vessels. Maritime Cybersecurity Assessment and Annex Guide (MCAAG)* shares three challenges for applying cybersecurity assessments and suggests three recommendations to address these challenges. One of these recommendations is to identify a cybersecurity officer (CySO). Eventually, MCAAG should be performed in the purview of an experienced cybersecurity expert. As a result, maritime organizations should find ways to involve senior leaders in risk assessment processes, as the methods described in the guidelines do not provide incentives to involve senior leaders.

The Implementation Guide for Cybersecurity on Vessels is easy to implement and adapt to different scopes. It also could allow the engagement of leadership to some extent. It has been prepared for vessels operating in the container industry; however, it can be applied to other MTSs. The guideline can be applied to perform risk analyses at tactical levels. We could not find any evidence proving the application of this guideline by an organization.

Among 48 scholarly papers listed in Table 4, none received an “Easy” score for the Implementability, Leadership Engagement, and Adaptability requirements. However, two articles received one “Moderate” and two “Easy” scores for these requirements. Paul et al. presented their method on a fictitious naval use case, demonstrating its flexibility for application beyond ships and naval contexts (Paul et al., 2021). Their risk analysis method focuses on assessing tactical-level risks. In a similar vein, Gunes et al. conducted a risk analysis on an actual port facility using a method designed for tactical-level risk assessment (Gunes et al., 2021). Both approaches are collaborative, enabling maritime professionals and stakeholders to actively participate in the risk assessment processes.

After analyzing 48 papers and 3 guidelines, it becomes apparent that the maritime sector requires a holistic cybersecurity risk analysis method that is not only easy to implement but also engages maritime leaders effectively. This method should readily adapt to various Maritime Transportation System (MTS) scopes, including vessels, ports, IT systems, and organizational processes. Furthermore, it should accommodate different levels of analysis, spanning both tactical and strategic perspectives. In response to these needs, we proposed CRAMMTS, a survey-based and collaborative cybersecurity risk analysis method, for the maritime sector.

4 Instrument Design and Pilot Study

In this section, we provide the details of the proposed risk analysis method we created to address the gaps in the literature. We named our risk analysis process Cyber Risk Assessment Method for Maritime Transportation Systems (CRAMMTS). CRAMMTS is an easy-to-implement and easy-to-customize survey-based risk analysis process that allows the participation of maritime leaders.

CRAMMTS risk model has been developed by customizing and extending the original ISRAM risk model. Customization and extensions to ISRAM risk model involves the alignment with IMO's guidelines and improvement of some survey parameters. ISRAM is a survey-based quantitative risk analysis method that helps assign weight values to survey questions and answer choices and converts the survey results into numerical values (Karabacak & Sogukpinar, 2005). ISRAM has been used by researchers and practitioners around the globe, evaluated by review articles, and credited by ENISA, The European Union Agency for Cybersecurity, as one of the major cyber risk analysis methods (European Union Agency for Cybersecurity, 2022).

Customizing and extending ISRAM risk model for the maritime sector's needs has been instrumental in filling the gaps in the literature. Refer to Table 5 for the details.

Table 5: Design goals and motivations for the risk analysis method to be proposed

Gap in the literature	**Our design goals and motivations**
Need for a tool that is easy to implement	CRAMMTS does not include complex mathematical and statistical methods. It helps convert qualitative questions describing complex situations into simple quantitative risk values.
Need for a tool that allows engagement of maritime leaders	CRAMMTS is a survey-based method, and the survey instrument allows the involvement of managers and policymakers.
Need for an adaptable tool	CRAMMTS is a flexible tool that can be used for different scopes, from a single ship to sector-wide assessments, from tactical-level analyses to strategical-level analyses. Moreover, survey-based CRAMMTS risk analysis processes can be integrated into existing risk analysis methods described in maritime risk assessment guidelines and risk management schemes.

Moreover, guidelines and recommendations of international organizations, governments, and NGOs have been thoroughly reviewed to make our survey and risk model compatible with the fundamental principles in those documents. Our survey-based risk analysis process and risk model help convert qualitative and different types of survey questions into quantitative yet simple risk values.

CRAMMTS has the following phases:

1) Phase 1: Survey preparation phase
    a. Phase 1.1: Identification of the themes
    b. Phase 1.2: Identification of the Impact and Likelihood factors
    c. Phase 1.3: Preparation of the survey questions and answer choices
2) Phase 2: Risk model preparation phase
    a. Phase 2.1: Identification of questions and answers' weights
    b. Phase 2.2: Customization of ISRAM risk model
    c. Phase 2.3: Preparation of normalization and risk tables
3) Phase 3: Survey phase
    a. Phase 3.1: Execution of the surveys
    b. Phase 3.2: Application of the risk model and calculation of the quantitative risk values

Figure 5 shows the flowchart of all these consecutive phases. In the survey preparation phase, we prepared 86 questions and answer choices to assess impact and likelihood factors. We determined weights for questions and answer choices, and finally, we conducted the survey. For upcoming CRAMMTS instances, organizations can use the existing questions, modify them, or add new questions to the pool. Moreover, they can change the weight values of questions and answer choices. In this regard, CRAMMTS allows the creation of a reusable survey infrastructure, and a maritime organization may start a survey within a determined scope with minimal customization of the survey infrastructure.

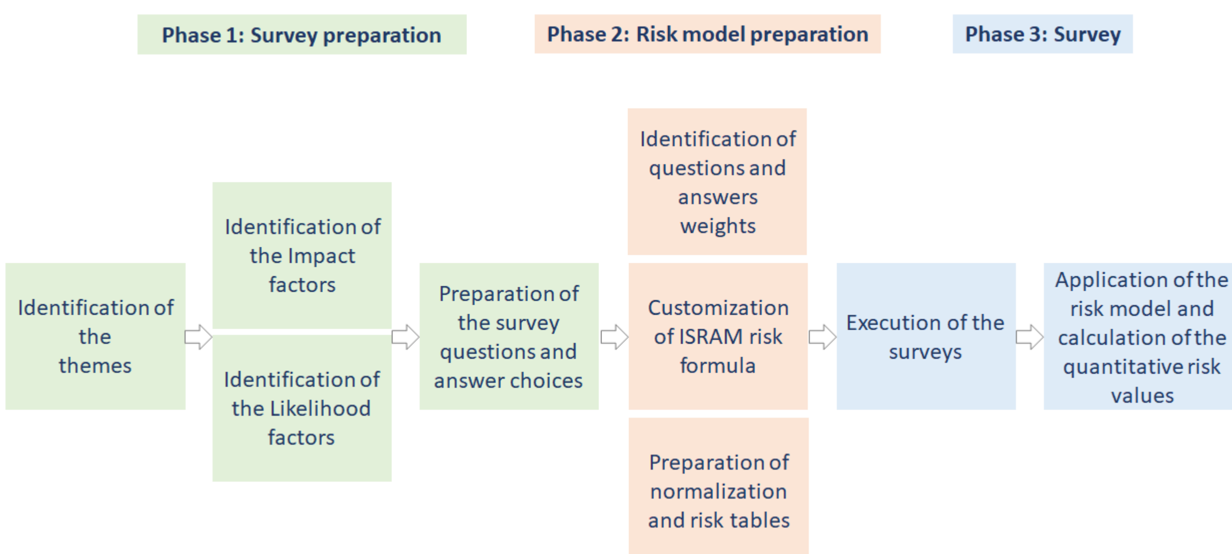

Figure 5: CRAMMTS risk analysis process

The following subsections provide the details of three main phases of the CRAMMTS risk analysis process in the context of our pilot surveys. We had the opportunity to send survey questions to a diverse set of maritime employees in seven different countries, thanks to the support of NATO Combined Joint Operations from the Sea Centre of Excellence.

The survey was initially sent to 80 professionals in the maritime sector using the Qualtrics tool, and the answers were collected anonymously. Forty-five professionals responded to the survey. Forty-five responses helped understand the collective risk perception of the maritime sector from the point of view of 45 maritime professionals.

4.1 Phase 1: Survey preparation

In the survey preparation phase, we decided to use two themes: threat-centric and asset-centric themes. We aimed to perform threat-centric and asset-centric risk evaluations based on survey results. We used various maritime resources, including gray literature and academic literature, to identify impact and likelihood factors for each theme. For example, we converted the security measures mentioned in maritime guidelines into impact/likelihood factors. Finally, we converted impact and likelihood factors into survey questions and proposed answer choices for each survey question.

The goal behind the threat-centric theme was to understand the risk perceptions of respondents through cyber threat-focused questions. We determined ten impact and ten likelihood factors for potential maritime cybersecurity incidents, each caused by a specific threat source.

The goal behind the asset-centric theme was to understand the risk perceptions of respondents through asset-focused questions. We determined twenty-two likelihood factors for potential cyber incidents for maritime platforms (ships, mobile offshore units) and port-related systems (including company offices); each factor corresponds to a specific MTS. We grouped impact factors into four for different types of assets. The bulleted list below summarizes the four groups of impact factors:

- Thirteen impact factors affecting maritime Information Technologies (IT), each corresponding to a specific information technology.
- Thirteen impact factors affecting maritime Operational Technologies (OT), each corresponding to a specific operational technology.
- Eight impact factors affecting maritime organizations, each corresponding to a specific organizational process.
- Eight impact factors affecting the maritime sector, each corresponding to a specific aspect of sectoral/national security.

Table 6 shows which themes were used to calculate the risk values. Specifically, we used 10 impact and 10 likelihood factors to assess the threat-centric risk. We performed four different asset-centric risk assessments, each corresponding to a different type of asset: (1) IT, (2) OT, (3) Organizational Processes, and (4) Sectoral and national security. We used the same likelihood factors for each group of assets; however, we used different impact factors for each group. The reason behind scrutinizing the asset-centric risk assessment was that the respondents mainly had years of experience in the maritime domain with an advanced understanding of different types of assets and were in various hierarchical positions in their organizations.

Table 6: Risk values for four different cases

Risk perception	**Impact and Likelihood factors used to assess the risk perception**
Threat-centric risk perception	Ten impact factors Ten likelihood factors
Asset-centric (Information Technologies) risk perception	Thirteen impact factors Twenty-two likelihood factors
Asset-centric (Operational Technologies) risk perception	Thirteen impact factors Twenty-two likelihood factors
Asset-centric (organizational processes) risk perception	Eight impact factors Twenty-two likelihood factors
Asset-centric (sectoral/national security) risk perception	Eight impact factors Twenty-two likelihood factors

In Phase 1 of CRAMMTS, we converted all impact and likelihood factors into survey questions. We determined answer choices for each question based on a 5-point Likert scale of agreement, importance, or likelihood, depending on the question type (See Table 8). As a result, we created two broad types of survey questions that fall into two broad themes: the questions that help determine the impact of an incident and the questions that help determine the likelihood of an incident. In Phase 3, these questions will assess respondents' impact and likelihood perceptions.

In addition to threat-centric and asset-centric themes, we could have included other themes in our pilot study. For example, other themes could be vulnerability-centric risk perception or compliance with specific maritime guidance. ISRAM could be customized to assess compliance with security standards and guidelines (Karabacak & Sogukpinar, 2006). Additional themes are not included because of the space constraints.

4.2 Phase 2: Risk model preparation

As with ISRAM, our risk model is based on Formula 1. Formula 1 states that risk is the combination of the likelihood of a threat event happening and the potential negative consequences if the event occurs (NIST, 2012). This formula is one of the fundamental cybersecurity risk models mainly used by academia, industry, and government.

$$\text{Risk} = \text{Impact} * \text{Likelihood}$$

Formula 1: Underlying risk model

Our risk model for converting cybersecurity survey results into a simple normalized risk value is shown in Formula 2. The first multiplier represents the impact value, whereas the second multiplier represents the likelihood value. This formula incorporates all survey parameters, including questions, answers, and participants.

$$Risk = \left[\frac{\sum_{i=1}^{p}\left(C_p \times M(\sum_{j=1}^{a} I_j T_j)\right)}{\sum_{i=1}^{p} C_p}\right] \times \left[\frac{\sum_{i=1}^{r}\left(C_r \times N(\sum_{j=1}^{b} L_j D_j)\right)}{\sum_{i=1}^{r} C_r}\right]$$

The first multiplier represents the Impact survey(s) (Produces a number between 1 and 5); refer to Table 11
The second multiplier represents the Likelihood survey(s) (Produces a number between 1 and 5); refer to Table 12
Risk: The numerical risk value (A number between 1 and 25), refer to Table 13 for categorization of values
p: The number of participants for the Impact survey
r: The number of participants for the Likelihood survey
a: The number of questions for the Impact survey, refer to Table 6
b: The number of questions for the Likelihood survey, refer to Table 6
I: The weight of the question-j for the Impact survey, refer to Table 7
T: The weight of the answer choice-j for a given question for the Impact survey, refer to Table 8
L: The weight of the question-j for the Likelihood survey, refer to Table 7
D: The weight of the answer choice-j for a given question for the Likelihood survey, refer to Table 8
M: Normalization operation for the Impact value, refer to Table 9
N: Normalization operation for the Likelihood value, refer to Table 10
C_x: Contribution factor of the survey respondent x, C is a number between 1 and 5, refer to Formula 3

Formula 2: CRAMMTS risk model

4.2.1 Weight values

We used Table 7 for the weight values of survey questions associated with Impact or Likelihood. This was not the case in our pilot survey study, but a factor could affect both Impact and Likelihood values. In this case, the question associated with the factor should be asked once in Phase 3 (CRAMMTS survey); however, both Impact and Likelihood factors should be included in calculations in Phase 2 (risk model preparation).

Table 7: Reference table for the question weight values

Weight of an Impact / Likelihood question (Possible values of I & L parameters in Formula 2)	Description
3	The factor significantly contributes to the Impact / Likelihood.
2	The factor moderately contributes to the Impact / Likelihood.

Weight of an Impact / Likelihood question (Possible values of I & L parameters in Formula 2)	Description
1	The factor marginally contributes to the Impact / Likelihood.

We used Table 8 for the weight values of answer choices.

Table 8: Reference table for the answer weight values

Weight of the answer choice	Description
5	The extremely influential answer choice. The answer choice has a significant impact on the Impact / Likelihood.
4	The very influential answer choice. The answer choice has an evident impact on the Impact / Likelihood.
3	The moderately influential answer choice. The answer choice has a moderate impact on the Impact / Likelihood.
2	The somewhat influential answer choice. The answer choice has a limited impact on the Impact / Likelihood.
1	The slightly influential answer choice. The answer choice has a marginal impact on the Impact / Likelihood.

4.2.2 Contribution factor

CRAMMTS risk model incorporates a Contribution Factor (C). The Contribution Factor aims to identify survey participants' knowledge and experience levels and reflect these on survey results. Specifically, the Contribution Factor increases the contribution of the experienced and confident participants to the survey and decreases the contribution of the inexperienced and relatively unconfident participants. We gathered information about the knowledge and experience levels of survey respondents with the help of three different types of demographic/generic questions. The details are as follows:

1. Group 1: Level of knowledge in Information and Communications Technology (ICT) and Cybersecurity (2 questions)
2. Group 2: Experience in the maritime domain (21 questions)
3. Group 3: Respondent's confidence level (1 question)

All 24 questions have answer choices based on a 5-point Likert scale. The answers to these questions are processed according to the Formula 3 to calculate the Contribution Factor in Formula 2.

The Contribution Factor for a survey respondent ranges from a minimum of one to a maximum of five, and it may include non-integer values.

$$C = Avg\left[\left(\frac{\sum_{j=1}^{2}(F1)_j}{2}\right) + \left(\frac{\sum_{j=1}^{21}(F2)_j}{21}\right) + F3\right]$$

C: Contribution factor for a given respondent, a number between 1 and 5 where 1means minimal and 5 means extensive knowledge and experience in ICT/cybersecurity or maritime domain
F1: The survey question to get the experience level in ICT and cybersecurity
F2: The survey question to get the experience level in the maritime domain
F3: The survey question to get the confidence level of the respondent
Avg: The arithmetic average of three parameters within the square brackets.

Formula 3: Contribution factor

4.2.3 Normalization operations

Normalization operations (M, N in Formula 2) convert bulk survey results for a specific respondent to a normalized value between 1 and 5. We prepared normalization tables specific to each survey to implement normalization operations. Each survey should have its specific normalization table regardless of the theme or the survey type (Impact or Likelihood).

For example, the normalization operations for the Impact and Likelihood surveys of the asset-centric (organizational processes) risk perception theme are implemented by the normalization tables shown in Table 9 and Table 10, respectively.

We used Formula *4* to find the minimum and maximum survey results for building normalization tables. The asset-centric (organizational processes) risk perception theme had 8 impact and 22 likelihood factors (see Table 6).

$$\sum_{j=1}^{a} I_j T_j \left\{ \begin{array}{c} \text{a: Total number of questions} \\ \text{I: The weight value of the j}^{\text{th}} \text{ question} \\ \text{T: The weight value of the selected answer choice for the j}^{\text{th}} \text{ question} \end{array} \right\}$$

Formula 4: Impact survey

Table 9 has been built by determining the maximum and minimum survey results for the Impact survey and then evenly grouping bulk survey results into five levels. More specifically, for the Impact survey, “a” was 8. The weight values for each Impact factor (I_j values) were already determined based on Table 7 (Three factors weighed as 3, two as 2, and three as 1). Maximum survey output is found by assuming that a participant chooses the most influential answer for all questions (so that T_j has its maximum possible value). In our case, the maximum survey output was 80, and the minimum survey output was 16.

Table 9: Normalization table for the Impact survey of asset-centric (organizational processes) risk perception theme

Bulk survey result	**Normalized value**
16 - 28	1
29 - 41	2
42 - 54	3
55 - 67	4
68 - 80	5

Table 10: Normalization table for the Likelihood survey of asset-centric (organizational processes) risk perception theme

Bulk survey result	**Normalized value**
47 - 84	1
85 - 122	2
123 - 160	3
161 -199	4
200 - 235	5

In our pilot study, we prepared 8 more normalization tables. Note that although we used the same Likelihood factors for all asset-centric themes, we used different weight values for some factors. That is why normalization tables were different. Because of space constraints, we did not share the remaining normalization tables in this publication.

Normalization operations ensure a value between 1 and 5 for the first and second multipliers of the CRAMMTS risk model shown in Formula 2. Therefore, the normalization operation is an abstraction layer between the survey infrastructure and the final normalized risk value, which will be between 1 and 25. Normalization operations also provide flexibility in survey design so that there are no restrictions on the number of questions, answer choices, weight values, and number of survey participants.

4.2.4 Representation of the risk

We were inspired by the IMO's guideline, “Revised Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-making Process,” for the Impact and Likelihood descriptions in Table 11 and Table 12 (IMO, 2018). Section 5.3 provides a detailed discussion of these descriptions and the corresponding scales for each description.

Table 11: Impact values and descriptions

Impact	Impact Description
4 < Impact ≤ 5	Catastrophic
3 < Impact ≤ 4	Severe
2 < Impact ≤ 3	Significant
1 < Impact ≤ 2	Moderate
0 < Impact ≤ 1	Minor

Table 12: Likelihood values and descriptions

Likelihood	Likelihood Description
4 < Likelihood ≤ 5	Almost certain
3 < Likelihood ≤ 4	Frequent
2 < Likelihood ≤ 3	Reasonably probable
1 < Likelihood ≤ 2	Remote
0 < Likelihood ≤ 1	Extremely remote

Formula 2 produces a risk value between 1 and 25. The authors categorized possible risk values into five groups; the second column of Table 13 shows descriptions for these categories. The third column of Table 13 shows the corresponding categories of risk based on IMO's revised guidelines for Formal Safety Assessment (FSA) (IMO, 2018).

Table 13: Risk values and descriptions

Risk = Impact * Likelihood	Risk description	IMO's risk description in the context of FSAs (Formal Safety Assessment)
20 ≤ Risk ≤ 25	Very high risk	Intolerable (Not acceptable)
15 ≤ Risk < 20	High risk	Intolerable (Not acceptable)
9 ≤ Risk < 15	Medium risk	ALARP (Acceptable, if made ALARP)
5 ≤ Risk < 9	Low risk	Negligible (Broadly Acceptable)
1 ≤ Risk < 5	Very low risk	Negligible (Acceptable)

The authors suggest the mapping between the risk descriptions in the second column of Table 13 and IMO's descriptions in the third column. ALARP in the third column stands for As Low As Reasonably Practicable. "Accidental events whose risks fall within ALARP region have to be reduced unless there is a disproportionate cost to the benefits obtained" (IMO, 2018). The risk values between 15 and 25 (inclusive) are considered intolerable risks. Intolerable risks have high likelihood and/or impact values. The associated action for intolerable risks is to act immediately.

The second group is the ALARP region, which has risk values between 9 (inclusive) and 15. Risk owners should prepare mitigation plans for these risks, which are medium-term at most. The third group of risks is negligible, with values between 1 (inclusive) and 9. There is no need to implement mitigations for these risks; however, they should be continuously watched for any changes in likelihood and impact factors.

Based on Table 6, five numerical risk values have been calculated using Formula 2: one threat-centric risk value and four asset-centric risk values for different types of assets. All risk values are normalized based on a scale of 1 to 25. 25 is the most severe risk with an impact of 5 and a likelihood of 5. 1 is the least severe risk with both impact and likelihood values "1".

Table 14 contains the descriptions of three categories of risks for one threat-centric and four asset-centric themes.

Table 14: Risk descriptions for each theme

Action	**Risk value**	**Threats-centric description**	**Asset-centric description (IT)**	**Asset-centric description (OT)**	**Asset-centric description (Organization)**	**Asset-centric description (Sector/nation)**
Act	15≤Risk≤25 (Intolerable)	Cyber threats (internal or external) can cause damage to maritime assets in the short term.	The functioning of IT systems can be damaged severely in the short-term	The functioning of OT systems can be damaged severely in the short-term	The functioning of organizational processes can be damaged severely in the short-term	National or sector-wide security can be damaged severely in the short-term
Plan	9 ≤ Risk < 15 (ALARP)	Cyber threats (internal or external) may cause damage to maritime assets in the medium term.	The functioning of IT systems might be degraded in the medium-term	The functioning of OT systems might be degraded in the medium-term	The functioning of organizational processes might be degraded in the medium-term	National or sector-wide security might be degraded in the medium-term
Watch	1-8 (Negligible)	Cyber threats (internal or external) may cause damage to maritime systems in the long term, depending on the changes in the internal and external environments.	The functioning of IT systems may be degraded in the long term depending on the changes in the internal and external environments.	The functioning of OT systems may be degraded in the long term depending on the changes in the internal and external environments.	Organizational processes may be degraded in the long term depending on the changes in the internal and external environments.	National or sector-wide security may be degraded in the long term depending on the changes in the internal and external environments.

The primary purpose of sharing simple quantitative risk values and grouping these values into three categories is to help policymakers understand the current security posture of the maritime domain in a simple, comprehensible, and repeatable way. The subsequent execution of the same survey will help create risk perception trends. Risk assessments performed by our risk model can positively contribute to a policy discussion, and quantitative values can help policymakers understand changes in the security posture over a given time span.

4.3 Phase 3: Survey

We executed the survey and obtained quantitative risk values at Phase 3 of the CRAMMTS. The survey was sent to 80 professionals in the maritime sector. The target group was chosen to get responses from a diverse set of respondents regarding hierarchical level in an organization, level of knowledge in the maritime sector, and level of knowledge in ICT and cybersecurity domains. Forty-five professionals responded to the survey, and this number of respondents achieved the targeted diversity. Figure 6 shows the distribution of the respondents according to their level of knowledge in information and communication technologies. 21% of respondents described themselves as having a high or very high level of experience in ICT. Almost 60% of the respondents had a moderate level of ICT knowledge—these three levels (very high, high, and moderate) sum up to 81%. Figure 6 also shows the distribution of the respondents based on their knowledge of cybersecurity. 45% of respondents considered themselves to have a high or moderate level of knowledge.

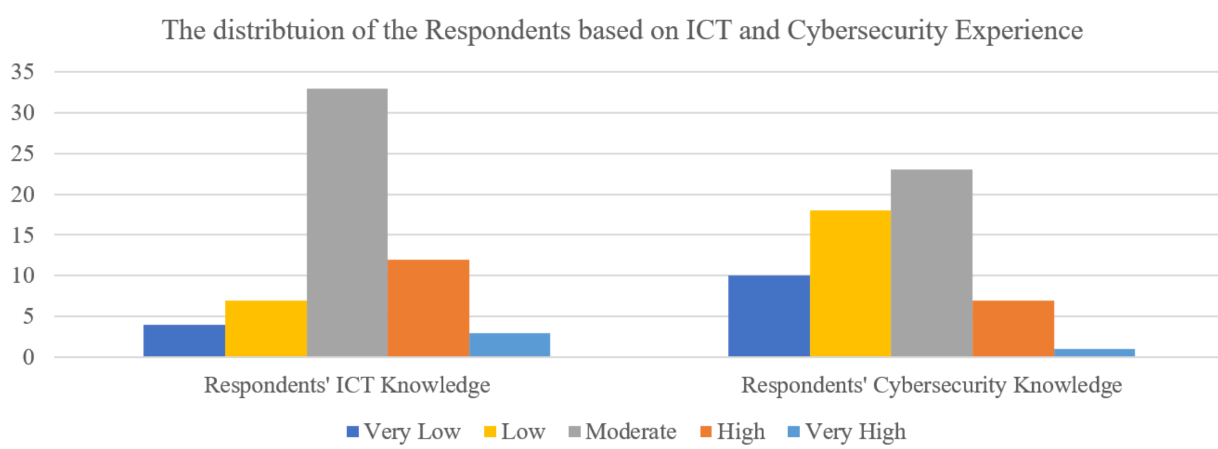

Figure 6: The distribution of the respondents based on their ICT and cybersecurity knowledge

According to Loomis et al., mitigating cyber risks in the maritime industry necessitates a collaborative effort among a broad range of stakeholders within the MTS (Loomis et al., 2021). Figure 7 shows the distributions of respondents according to their specific area within the maritime sector. The respondents were from diverse sectors, including but not limited to the public sector, military, environment, law enforcement, and shipping. The respondents' average experience in the maritime domain was 10+ years.

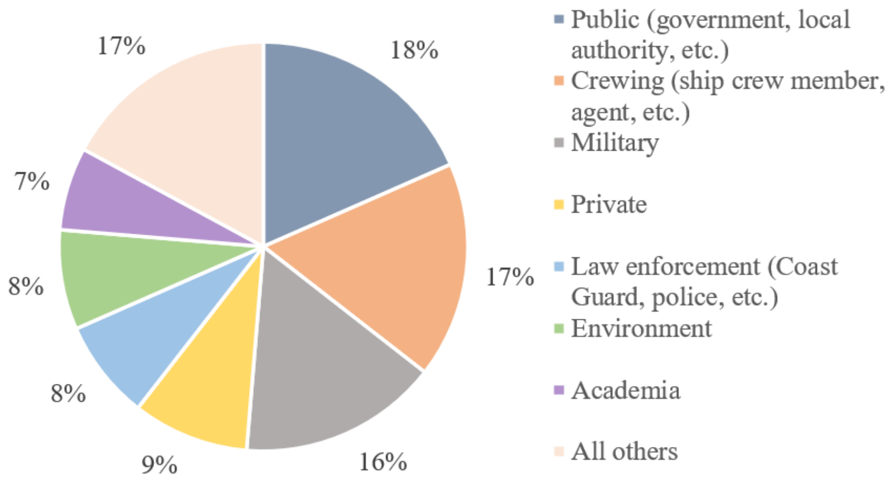

Figure 7: The distributions of respondents based on their specific area within the maritime sector

Figure 8 shows the distribution of the hierarchical levels of respondents. 43.24% of respondents were operators, officers, and mid-level managers. 40.54% were at the operational management level, such as ship management and commanding officer. 10.81% of the respondents were top-level managers.

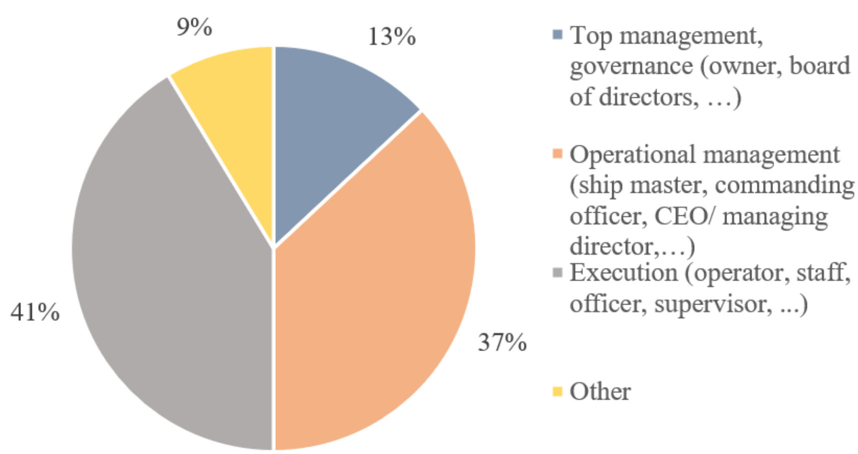

Figure 8: The distribution of the hierarchical levels of respondents

The risk values for each theme are shown in Table 15. There is no Very High level of risk among the five themes. Risk levels for the first four themes are High. In contrast, the risk level for the last theme, which is the Asset-centric (sectoral and national security) theme, is Medium based on the categorization of Table 13. The matter of fact is that asset-centric risk values are close to each other; they all can be considered Medium-level. Table 15 demonstrates that a risk analysis process involving questions regarding cyber threat actors produces a higher risk value than the risk analysis process involving questions regarding asset values.

The risk values for IT assets and OT assets are very close, although their impact and likelihood values differ. The impact value associated with OT assets is higher than that associated with IT assets. In contrast, the likelihood value for OT assets is lower than the likelihood value for IT assets. This result is expected; the impact of an OT system breach could directly affect the environment and human life. However, the likelihood is lower because these systems are more isolated compared to IT systems.

Based on the risk values in Table 15, risk owners should immediately act to mitigate risks in maritime assets at different levels, including IT, OT, and organizational processes. For the sectoral and national security theme, the risk is at the border of high-level risk, so mitigation actions should be planned.

Table 15: Risk values for four different cases

Theme	Impact	Likelihood	Risk	Risk description (Ref: Table 13)	Risk description (Ref: Table 14)	Action (Ref: Table 14)
Threat-centric theme	4.25	4.25	18.06	High	Intolerable	Act
Asset-centric (IT) theme	3.95	3.93	15.52	High	Intolerable	Act
Asset-centric (OT) theme	4.22	3.70	15.61	High	Intolerable	Act
Asset-centric (organizational security) theme	4.07	3.88	15.79	High	Intolerable	Act
Asset-centric (sectoral and national security) theme	3.91	3.75	14.66	Medium	ALARP	Plan

5 Discussion

Our discussion section is divided into four distinct parts. Initially, we delve into how CRAMMTS tackles various maritime cybersecurity risk assessment challenges that have been highlighted in academic research. Next, we explore the specifics of how we have aligned CRAMMTS with the International Maritime Organization's (IMO) Cyber Risk Management Guidelines. In the third part, we provide the details of our improvements for IMO's categorizations of severity, frequency, and risk values and how we incorporated the improvements in CRAMMTS. Finally, the last part focuses on how the Eisenhower matrix aids in prioritizing mitigation strategies.

5.1 How CRAMMTS Addresses the Challenges of Maritime Cybersecurity Risk Assessment

Bolbot, Kulkarni, et al. composed a list of challenges for cybersecurity risk assessment processes in the maritime sector by reviewing 18 academic papers (Bolbot, Kulkarni, et al., 2022). Drummond and Machado answered the research question: “What technical challenges are found when implementing cyber risk management procedures in ports?” (Drummond & Machado, 2021). Table 16 shows these challenges and how CRAMMTS addresses some of these challenges.

Table 16: Cybersecurity risk assessment challenges in the maritime sector

Risk assessment processes challenges (Bolbot, Kulkarni, et al., 2022; Drummond & Machado, 2021)	**How CRAMMTS addresses the challenge, if applicable**
The difficulty with accurate prioritization of cyberattack scenarios due to the lack of accurate historical cyber incidents information to support credible cyber risk assessments	CRAMMTS surveys help build a history of cyber incidents.
Unknown interactions between systems and risk factors	N/A
The cost of having a diverse group of experts in risk assessments	CRAMMTS risk assessment process does not require the involvement of experts. The survey preparation process may require expert consultancy, but this will not be costly.
The constantly evolving nature of the area, considering the long lifecycle of ships	CRAMMTS surveys can be customized based on the changes in the area.
Diversity of marine equipment suppliers	CRAMMTS risk assessment model can be tailored by adding more questions about equipment from different suppliers.
The transferability of results of one risk assessment	The results of each risk assessment can be transferred into qualitative values along with detailed descriptions of each scenario or even to monetary values by the help of some reference conversion tables.
Having efficient, not resource-intensive risk assessment	The CRAMMTS risk assessment method is generally not demanding in terms of resources. While the initial setup of the survey might require some effort, especially if starting from scratch, subsequent preparations are much simpler, involving just updates to the existing survey. After the initial survey is set up, conducting it requires minimal resources.
Ensuring sufficient communication amongst various stakeholders during risk assessment	CRAMMTS surveys can be answered individually or by a group of people; in this way, CRAMMTS can be used as an enabler of communications amongst different stakeholders.
Identifying the effects of connectivity and complex cyberattacks (accurately representing the operational and information technologies in ships and the relevant temporal and functional relationships)	CRAMMTS risk assessment surveys can be easily tailored to include more questions about operational and information technologies and the relevant temporal and functional relationships between them.

Risk assessment processes challenges (Bolbot, Kulkarni, et al., 2022; Drummond & Machado, 2021)	**How CRAMMTS addresses the challenge, if applicable**
The lack of efficient cybersecurity metrics	CRAMMTS enables the incorporation of the cybersecurity metrics identified in the standards into risk analysis surveys
Model-based approaches require significant computational power for their application associated with state-space growth.	CRAMMTS is not a model-based approach and does not require the use of specialized software or simulation tools
Lack of credible and commonly agreed risk acceptance criteria for cyber risk	CRAMMTS incorporates the IMO's risk categorization and acceptance criteria. See section 5.2 for details.
The selection of appropriate scales for risk ranking	CRAMMTS provides a precise and repeatable method for scaling impact, likelihood, and risk values.
Difficulty establishing uniform standards, Challenges in creating and applying standardized processes that can flexibly accommodate different environments.	CRAMMTS is a promising method for standardizing the risk assessment process; it has a robust risk model and a well-defined survey preparation process.
Uncertainty in defining the entity responsible for assessments	N/A
Substantial funds are required for training and hiring qualified professionals to adapt standardized processes to varied environments and ongoing training demands for staff.	CRAMMTS might reduce the cost of risk and security assessment training.

5.2 Alignment with Sectoral Guidelines

Ensuring that a maritime cyber risk analysis method aligns with industry guidelines is important, as these guidelines may be mandated by regulatory agencies or utilized for various other purposes, such as benchmarking. CRAMMTS has been aligned with the International Maritime Organization's (IMO) "Revised Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-making Process." This alignment includes similarities in Impact and Likelihood descriptions, Risk categorization, as well as options and priorities for risk mitigation. For a detailed explanation of how this alignment was achieved, please refer to Section 4.2.

Our CRAMMTS survey application was aligned with several recommendations provided by IMO's Guidelines on Maritime Cyber Risk Management (IMO, 2021). IMO recommends that organizations consider the distinction between the Information Technology (IT) and Operational Technology (OT) systems in the Guidelines on Maritime Cyber Risk Management**.** The cybersecurity survey has separate questions to assess the impact levels of security incidents on IT and OT systems. Separate risk values have been calculated for IT and OT systems.

Section 1.1 of the IMO cyber risk management guideline emphasizes assets and threats and mentions the potential impacts of cyber incidents. The emphasis on assets and threats was realized in the cybersecurity survey by having both threat-centric and asset-centric themes.

Section 2.1.4 of the cyber risk management guideline suggests including external and internal threats. Our threat-centric questions include both types of threat actors.

Lastly, IMO guidelines mention the importance of the inclusion of top-level management and a breadth-based approach within an organization, stating "Effective cyber risk management should start at the senior management level" and "Effective cyber risk management should ensure an appropriate level of awareness of cyber risks at all levels of an organization. The level of awareness and preparedness should be appropriate to roles and responsibilities in the cyber risk management system." Top-level managers were among the survey participants, and the organizations were well represented by the participants across various hierarchies, from the top-level management to the crew level.

5.3 Improving IMO's Severity, Frequency, and Risk Indexes

IMO's Revised Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-making Process is an annex that suggests reference tables for the Impact and Likelihood values (IMO, 2018). The guideline uses the "Severity" and "Frequency" keywords in place of "Impact" and "Likelihood". The definition of risk is "the combination of the frequency and the severity of the consequence (IMO, 2018)." The revised guideline suggests logarithmic scales for the Impact and Likelihood categorizations. IMO's FSA uses the values 1 to 4 for the Impact levels and 1, 3, 5, and 7 for the Likelihood levels. Because of the use of logarithmic scales, the guideline suggests calculating the risk value by adding the Impact and Likelihood values. The four levels for the Severity value are Minor, Significant, Severe, and Catastrophic. The four levels for Frequency are Extremely Remote, Remote, Reasonable probable, and Frequent.

In our opinion, there is a major gap between "Minor" and "Significant" for the Severity value. For the Likelihood value, there could be a fifth value to represent events with a likelihood higher than "Frequent." Our study used five levels for Impact and Likelihood values of cyber risks. We added a "Moderate" impact value between the "Minor" and "Significant" values suggested in the IMO publication. We added "Almost Certain" as the fifth frequency level after "Frequent". Our study implemented a more widely used risk calculation method in information security literature. We did not use logarithmic scales. In this regard, we multiplied the impact and likelihood values scaled between 1 and 5. Refer to Section 4.2 for the proposed Impact, Likelihood, and Risk tables.

5.4 Discussion on Prioritization of Mitigations

Although numerous risk factors vary in severity and impact, resources available to address these risks are often limited. Therefore, an analytical and practical approach to prioritizing mitigation efforts is essential. The Eisenhower Matrix is a simple time management tool that can help individuals and organizations prioritize tasks based on their urgency and importance. The matrix was popularized by former US president Dwight D. Eisenhower. There are many scholarly articles that implement the matrix in different settings. In this section, we showed how the Eisenhower decision matrix can be used to categorize the IMO's mitigation actions (Act, Plan, and Watch) based on risk levels in Table 14. The actions are shown in Table 17, which is an instance of the popular Eisenhower decision matrix.

In the original matrix, two features are associated with each task: urgency and importance. Tasks that are both urgent and important are performed; those that are not urgent but important are planned; tasks that are urgent but not important are delegated; and, finally, tasks that are neither urgent nor important are eliminated.

In cyber risk management, urgency can be represented by the likelihood of potential cyber incidents. Importance can be represented by the impact of potential cyber incidents. In this regard, high-impact and highly likely incidents should be acted upon immediately. Mitigation steps should be planned for high impact & less likely and low impact & highly likely cyber incidents. Finally, low-impact and low-frequency cyber incidents should be observed for potential changes in likelihood and impact factors.

Table 17: Eisenhower Decision Matrix with a mapping to IMO actions (Act, Plan, Watch)

	Urgent (High-frequency incidents)	**Not Urgent (Low-frequency incidents)**
Important (High impact incidents)	Immediately act for intolerable risk	Plan for tolerable risks
Not Important (Low impact incidents)	Plan for tolerable risks	Watch negligible risks

6 Conclusion

Digitalization of MTS made cybersecurity risks an integral part of safety in the maritime sector. Despite this, managers and policymakers in the maritime domain have yet to gain sufficient depth of knowledge in information technologies and cybersecurity. In addition, a limited number of comprehensive cybersecurity risk analysis methods cover various levels of maritime systems and organizational hierarchies. Consequently, top-level managers could not perform risk-informed decision-making. However, cybersecurity risk analysis should be the responsibility of an organization's top-level management rather than being immediately delegated to the ship security officers or the IT department head (Kessler & Shepard, 2022, 2024AU; Mission Secure, 2021).

CRAMMTS is a survey-based risk analysis tool designed for MTS. CRAMMTS incorporates survey preparation, risk model preparation, and survey execution phases. It does not include complex mathematical and statistical tools as it is based on ISRAM. Our method allows the participation of maritime employees in cybersecurity risk analysis processes. In our pilot risk analysis study, we executed a maritime cybersecurity survey. We converted the opinions of respondents into simple quantitative values to represent the perceptions of maritime professionals as risk values.

One of the main motivations behind using ISRAM as the risk model is that policymakers and top-level managers frequently want to see percentages or simple normalized values instead of executive summaries and long paragraphs. We proposed a model to quantify the survey results to help policymakers comprehend the general security posture of the maritime domain. This approach efficiently provides them with the needed information, such as helping policymakers comprehend the general security posture of the maritime domain and helping them understand the changes over time to analyze trends. Maritime organizations should find ways to involve senior leaders in risk assessment processes, as risk assessment methods described in the maritime guidelines prepared by governments and NGOs do not provide incentives to involve senior leaders. With the help of CRAMMTS, policymakers and top-level managers not only consume the risk results but also become contributors to the risk analysis processes through the customization of ISRAM.

The study has some unique features. First, we covered different scopes (IT, OT, organizational processes, sectoral/national security) using a comprehensive set of survey questions. Second, we used a survey methodology to encompass strategic and tactical levels in the maritime domain. Our method can easily be integrated into existing risk management guidelines thanks to the ease of application and repeatability. Our customized risk model inherits the advantages of ISRAM: easy to comprehend, cost-effective, and does not require special software, flexible, and frequently used in practical applications to support risk-informed decision making.

References

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity Challenges in the Maritime Sector. *Network*, *2*(1), Article 1. https://doi.org/10.3390/network2010009

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, *45*, 547–554. https://doi.org/10.1016/j.trpro.2020.03.058

Amro, A., & Gkioulos, V. (2023a). Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. *International Journal of Information Security*, *22*(1), 249–288. https://doi.org/10.1007/s10207-022-00638-y

Amro, A., & Gkioulos, V. (2023b). Evaluation of a Cyber Risk Assessment Approach for Cyber–Physical Systems: Maritime- and Energy-Use Cases. *Journal of Marine Science and Engineering*, *11*(4), 744. https://doi.org/10.3390/jmse11040744

Amro, A., Kavallieratos, G., Louzis, K., & Thieme, C. A. (2020). Impact of cyber risk on the safety of the MilliAmpere2 Autonomous Passenger Ship. *IOP Conference Series: Materials Science and Engineering*, *929*(1). https://doi.org/10.1088/1757-899X/929/1/012018

Andrews, D. J., Pennetti, C. A., Collier, Z. A., Polmateer, T. L., & Lambert, J. H. (2020). Systems Evaluation for Defense Operations of Maritime Transport. *2020 IEEE International Systems Conference (SysCon)*, 714–720. https://doi.org/10.1109/SysCon47679.2020.9275887

A.P. Moller - Maersk. (2017). *A.P. Moller—Maersk Interim Report Q2 2017*. https://investor.maersk.com/static-files/7eee21c8-e825-46d2-bc62-dcd155d00e88

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2022). A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Transactions on Intelligent Transportation Systems*, 1–14. https://doi.org/10.1109/TITS.2022.3164678

Baggott, S. S., & Santos, J. R. (2020). A Risk Analysis Framework for Cyber Security and Critical Infrastructure Protection of the U.S. Electric Power Grid. *Risk Analysis: An International Journal*, *40*(9). https://doi.org/10.1111/risa.13511

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. *Information*, *13*(1), 22. https://doi.org/10.3390/info13010022

Bergman, B. (2021, July 29). *Systematic data analysis reveals false vessel tracks*. SkyTruth. https://skytruth.org/2021/07/systematic-data-analysis-reveals-false-vessel-tracks/

Bernsmed, K., Froystad, C., Meland, P. Há., Nesheim, D. A., & Rodseth, O. J. (2018). Visualizing Cyber Security Risks with BowTie Diagrams. *Graphical Models for Security*, *10744*. https://doi.org/10.1007/978-3-319-74860-3

BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass), & World Shipping Council (WSC). (2020). *The Guidelines on Cyber Security Onboard Ships*. https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

BIMCO, & International Chamber of Shipping. (2024). *Cyber Security Workbook for On Board Ship Use* (5th Edition). Witherby Publishing Group Ltd.

Bolbot, V., Basnet, S., Zhao, H., Valdez Banda, O., & Silverajan, B. (2022). *Investigating a novel approach for cybersecurity risk analysis with application to remote pilotage operations*. https://doi.org/10.5281/ZENODO.7143998

Bolbot, V., Kulkarni, K., Brunou, P., Banda, O. V., & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*, *39*, 100571. https://doi.org/10.1016/j.ijcip.2022.100571

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2019). *Safety related cyber-attacks identification and assessment for autonomous inland ships*. 15.

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. *Safety Science*, *131*, 104908. https://doi.org/10.1016/j.ssci.2020.104908

Bolbot, V., Theotokatos, G., Wennersberg, L., Faivre, J., Vassalos, D., Boulougouris, E., Jan Rødseth, Ø., Andersen, P., Pauwelyn, A.-S., & Van Coillie, A. (2023). A novel risk assessment process: Application to an autonomous inland waterways ship. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, *237*(2), 436–458. https://doi.org/10.1177/1748006X211051829

Chang, C.-H., Kontovas, C., Yu, Q., & Yang, Z. (2021). Risk assessment of the operations of maritime autonomous surface ships. *Reliability Engineering & System Safety*, *207*, 107324. https://doi.org/10.1016/j.ress.2020.107324

Chubb, N., Finn, P., & Daniel Ng. (2022). *THE GREAT DISCONNECT: The state of cyber risk management in the maritime industry*. Thetius.

Crisis Group. (2023, November 5). *Strait of Hormuz*. https://www.crisisgroup.org/trigger-list/iran-us-trigger-list/flashpoints/hormuz

DCSA. (2020). *DCSA Implementation Guide for Cyber Security on Vessels v1.0*. https://dcsa.org/wp-content/uploads/2020/03/DCSA-Implementation-Guideline-for-BIMCO-Compliant-Cyber-Security-on-Vessels-v1.0.pdf

De Peralta, F. A., Gorton, A. M., Watson, M. D., Bays, R. M., Boles, J. R., Gorton, B. T., Castleberry, J. E., & Powers, F. E. (2020). Cybersecurity Resiliency of Marine Renewable Energy Systems- Part 1: Identifying Cybersecurity Vulnerabilities and Determining Risk. *Marine Technology Society Journal*, *54*(6), 97–107. https://doi.org/10.4031/MTSJ.54.6.9

De Peralta, F. A., Watson, M. D., Bays, R. M., Boles, J. R., & Powers, F. E. (2021). Cybersecurity Resiliency of Marine Renewable Energy Systems Part 2: Cybersecurity Best Practices and Risk Management. *Marine Technology Society Journal*, *55*(2), 104–116. https://doi.org/10.4031/MTSJ.55.2.4

Drummond, B. M., & Machado, R. C. S. (2021). Cyber Security Risk Management for Ports—A Systematic Literature Review. *2021 International Workshop on Metrology for the Sea; Learning to Measure Sea Health Parameters (MetroSea)*, 406–411. https://doi.org/10.1109/MetroSea52177.2021.9611569

ENISA. (2020). *Cyber Risk Management for Ports: Guidelines for cybersecurity in the maritime sector*.

European Union Agency for Cybersecurity. (2022). *Compendium of Risk Management Frameworks with Potential Interoperability: Supplement to the Interoperable EU Risk Management Framework Report*. Publications Office. https://data.europa.eu/doi/10.2824/75906

Farah, M. B., Al-Kadri, M. O., Ahmed, Y., Abouzariba, R., & Bellekens, X. (2023). Cyber Incident Scenarios in the Maritime Industry: Risk Assessment and Mitigation Strategies. *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, 194–199. https://doi.org/10.1109/CSR57506.2023.10224972

Grobarcik, D., Loomis, W., Poznansky, M., & Smith, F. (2022). *Wargaming to Find a Safe Port in a Cyber Storm*.

Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. *Computers & Security*, *103*, 102196. https://doi.org/10.1016/j.cose.2021.102196

Harrington, K. (2013, March 7). *Malware Infects Gulf of Mexico Offshore Rigs*. American Institute of Chemical Engineers. https://www.aiche.org/chenected/2013/03/malware-infects-gulf-mexico-offshore-rigs

Harris, M. (2021, July 29). Phantom Warships Are Courting Chaos in Conflict Zones. *Wired*. https://www.wired.com/story/fake-warships-ais-signals-russia-crimea/

Hemminghaus, C., Bauer, J., & Padilla, E. (2021). BRAT: A BRidge Attack Tool for Cyber Security Assessments of Maritime Systems. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, *15*(1), 35–44. https://doi.org/10.12716/1001.15.01.02

IACS. (2022). *Recommendation on Cyber Resilience (IACS Rec. 2020/Corr.2 2022)*. IACS.

IMO. (2018). *Revised guidelines for formal safety assessment (FSA) for use in the IMO rule-making process*.

IMO. (2021). *Guidelines on Maritime Cyber Risk Management*. https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf

Informa. (2020, September 28). *CMA CGM confirms ransomware attack*. Lloyd's List. https://lloydslist.maritimeintelligence.informa.com/LL1134044/CMA-CGM-confirms-ransomware-attack

Iphar, C., Napoli, A., & Ray, C. (2020). An expert-based method for the risk assessment of anomalous maritime transportation data. *Applied Ocean Research*, *104*, 102337. https://doi.org/10.1016/j.apor.2020.102337

ISO. (2013). *ISO - ISO/IEC 27001—Information security management*.

ISO. (2018). *ISO 31000 Risk Management, Guidelines*. ISO.

Jacq, O., Boudvin, X., Brosset, D., Kermarrec, Y., & Simonin, J. (2018). Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre. *2018 2nd Cyber Security in Networking Conference (CSNet)*, 1–8. https://doi.org/10.1109/CSNET.2018.8602669

Jacq, O., Salazar, P. G., Parasuraman, K., Kuusijarvi, J., Gkaniatsou, A., Latsa, E., & Amditis, A. (2021). The Cyber-MAR Project: First Results and Perspectives on the Use of Hybrid Cyber Ranges for Port Cyber Risk Assessment. *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 409–414. https://doi.org/10.1109/CSR51186.2021.9527968

Kalogeraki, E.-M., Papastergiou, S., Mouratidis, H., & Polemi, N. (2018). A Novel Risk Assessment Methodology for SCADA Maritime Logistics Environments. *Applied Sciences*, *8*(9), 1477. https://doi.org/10.3390/app8091477

Kapadia, S. (2020, April 29). *3 years, 3 cyberattacks on major ocean carriers. How can shippers protect themselves?* Supply Chain Dive. https://www.supplychaindive.com/news/ocean-carrier-cybersecurity-maersk-msc-cosco/576754/

Karabacak, B., & Sogukpinar, I. (2005). ISRAM: Information security risk analysis method. *Computers & Security*, *24*(2), 147–159. https://doi.org/10.1016/j.cose.2004.07.004

Karabacak, B., & Sogukpinar, I. (2006). A quantitative method for ISO 17799 gap analysis. *Computers & Security*, *25*(6), 413–419. https://doi.org/10.1016/j.cose.2006.05.001

Kavallieratos, G., Spathoulas, G., & Katsikas, S. (2021). Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems. *Sensors*, *21*(5), 1691. https://doi.org/10.3390/s21051691

Kayisoglu, G., Bolat, P., & Tam, K. (2022). Evaluating SLIM-based human error probability for ECDIS cybersecurity in maritime. *Journal of Navigation*, *75*(6), 1364–1388. https://doi.org/10.1017/S0373463322000534

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*, *37*, 100526. https://doi.org/10.1016/j.ijcip.2022.100526

Kessler, G. C. (2020). *Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity*. *14*(2), 279–285. https://doi.org/10.12716/1001.14.02.02

Kessler, G. C. (2023). *AIS research using a Raspberry Pi*. https://www.garykessler.net/library/ais_pi.html

Kessler, G. C., & Shepard, S. D. (2022). *Maritime Cybersecurity: A Guide for Leaders and Managers*.

Kessler, G. C., & Shepard, S. D. (2024). *Maritime Cybersecurity A Guide for Leaders and Managers Second Edition (v2.2, 01/2024)*. https://www.garykessler.net/MaritimeCybersecurityBook/index.html

Kovacks, E. (2023, November 13). *Operations at Major Australian Ports Significantly Disrupted by Cyberattack*. https://www.securityweek.com/operations-at-major-australian-ports-significantly-disrupted-by-cyberattack/

Kuhn, K., Bicakci, S., & Shaikh, S. A. (2021). COVID-19 digitization in maritime: Understanding cyber risks. *WMU Journal of Maritime Affairs*, *20*(2), 193–214. https://doi.org/10.1007/s13437-021-00235-1

Lampreia, S., Lobo, V., & Vairinhos, V. (2022). *Cybersecurity Risk Assessment: The Ship Maintenance Databases' Case Study*. *5*(2).

LeBlanc, J. (2021). Suez Canal Blockage: Ripple Effect on Miami Valley Supply Chain. *Business Administration Faculty Contributions to the Popular Press*. https://digitalcommons.cedarville.edu/business_administration_media_contributions/120

Lee, J. M., & Wong, E. Y. (2021). Suez Canal blockage: An analysis of legal impact, risks and liabilities to the global supply chain. *MATEC Web of Conferences*, *339*, 01019. https://doi.org/10.1051/matecconf/202133901019

Li, X., Oh, P., Zhou, Y., & Yuen, K. F. (2023). Operational risk identification of maritime surface autonomous ship: A network analysis approach. *Transport Policy*, *130*, 1–14. https://doi.org/10.1016/j.tranpol.2022.10.012

Liang, A. (2023, November 13). *DP World: Australia sites back online after cyber-attack*. https://www.bbc.com/news/business-67400164

Loomis, W., Singh, V. V., Kessler, G. C., & Bellekens, X. (2021). *Raising the colors: Signaling for cooperation on maritime cybersecurity*. Atlantic Council.

Lopez, E. (2018, July 31). *How COSCO responded to a cyberattack on its systems*. Supply Chain Dive. https://www.supplychaindive.com/news/COSCO-cyberattack-response-timeline/529008/

Maritime Commons. (2015, June 15). *6/15/2015: Coast Guard Commandant on Cyber in the maritime domain*. Maritime Commons. https://mariners.coastguard.blog/2015/06/15/6152015-coast-guard-commandant-on-cyber-in-the-maritime-domain/

Mathews, L. (2017, August 16). *NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million*. Forbes. https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/

Meland, P. Há., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A Retrospective Analysis of Maritime Cyber Security Incidents. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, *15*(3), 519–530. https://doi.org/10.12716/1001.15.03.04

Melnyk, O., Onyshchenko, S., Onishchenko, O., Shumylo, O., Voloshyn, A., Koskina, Y., & Volianska, Y. (2022). Review of Ship Information Security Risks and Safety of Maritime Transportation Issues. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, *16*(4), 717–722. https://doi.org/10.12716/1001.16.04.13

Melnyk, O., Onyshchenko, S., Pavlova, N., Kravchenko, O., & Borovyk, S. (2022). Integrated Ship Cybersecurity Management as a Part of Maritime Safety and Security System. *International Journal of Computer Science and Network Security*, *22*(3), 135–140. https://doi.org/10.22937/IJCSNS.2022.22.3.18

Millefiori, L. M., Braca, P., Zissis, D., Spiliopoulos, G., Marano, S., Willett, P. K., & Carniel, S. (2021). COVID-19 impact on global maritime mobility. *Scientific Reports*, *11*(1), Article 1. https://doi.org/10.1038/s41598-021-97461-7

Mission Secure. (2021). *A Comprehensive Guide to Maritime Cybersecurity*.

MSC. (2020, April 15). *Network Outage Resolved*. MSC. https://www.msc.com/en/newsroom/news/2020/april/network-outage-resolved

Nguyen, S., Shu-Ling Chen, P., & Du, Y. (2022). Risk assessment of maritime container shipping blockchain-integrated systems: An analysis of multi-event scenarios. *Transportation Research Part E: Logistics and Transportation Review*, *163*, 102764. https://doi.org/10.1016/j.tre.2022.102764

NHL Stenden. (2024). *Maritime Cyber Attack Database (MCAD)*. https://maritimecybersecurity.nl

Niemiec, M., Pappalardo, S. M., Bozhilova, M., Stoianov, N., Dziech, A., & Stiller, B. (2022). Multi-sector Risk Management Framework for Analysis Cybersecurity Challenges and Opportunities. *Multimedia Communications, Services and Security*, *1689*. https://doi.org/10.1007/978-3-031-20215-5

NIST. (2012). *Guide for conducting risk assessments* (NIST SP 800-30r1; 0 ed., p. NIST SP 800-30r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

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

Patterson, D. A., & Bridgelall, R. (2020). Attack risk modelling for the San Diego maritime facilities. *Marine Policy*, *121*, 104210. https://doi.org/10.1016/j.marpol.2020.104210

Paul, S., Naouar, D., & Gureghian, E. (2021). Obérisk: Cybersecurity Requirements Elicitation through Agile Remote or Face-to-Face Risk Management Brainstorming Sessions. *Information*, *12*(9), 349. https://doi.org/10.3390/info12090349

Pavlinovic, M., Racic, M., & Karin, I. (2022). Cyber Risks in Maritime Industry – Case Study of Croatian Seafarers. *Human Interaction, Emerging Technologies and Future Systems V*, *319*, 108–113.

Pijpker, J., & McCombie, S. J. (2023). A Ship Honeynet to Gather Cyber Threat Intelligence for the Maritime Sector. *2023 IEEE 48th Conference on Local Computer Networks (LCN)*, 1–6. https://doi.org/10.1109/LCN58197.2023.10223347

Polatidis, N., Pavlidis, M., & Mouratidis, H. (2018). Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards & Interfaces*, *56*, 74–82. https://doi.org/10.1016/j.csi.2017.09.006

Pöyhönen, J. (2022). Cybersecurity risk assessment subjects in information flows. *European Conference on Cyber Warfare and Security*, *21*(1), 222–230. https://doi.org/10.34190/eccws.21.1.263

Pöyhönen, J. (2023). Assessment of Cyber Security risks: A Smart Terminal Process. *European Conference on Cyber Warfare and Security*, *22*(1), 366–373. https://doi.org/10.34190/eccws.22.1.1060

Pöyhönen, J., & Lehto, M. (2022). Assessment of Cybersecurity Risks: Maritime Automated Piloting Process. *International Conference on Cyber Warfare and Security*, *17*(1), 262–271. https://doi.org/10.34190/iccws.17.1.18

Progoulakis, I., Nikitakos, N., Dalaklis, D., Christodoulou, A., Dalaklis, A., & Yaacob, R. (2023). Digitalization and Cyber Physical Security Aspects in Maritime Transportation and Port Infrastructure. In T. M. Johansson, D. Dalaklis, J. E. Fernández, A. Pastra, & M. Lennan (Eds.), *Smart Ports and Robotic Systems* (pp. 227–248). Springer International Publishing. https://doi.org/10.1007/978-3-031-25296-9_12

Rajaram, P., Goh, M., & Zhou, J. (2022). Guidelines for cyber risk management in shipboard operational technology systems. *Journal of Physics: Conference Series*, *2311*(1), 012002. https://doi.org/10.1088/1742-6596/2311/1/012002

Roberts, F. S., Egan, D., Nelson, C., & Whytlaw, R. (2019). Combined Cyber and Physical Attacks on the Maritime Transportation System. *NMIOTC Maritime Interdiction Operations Journal*, *18*, 27–37.

Schauer, S., Polemi, N., & Mouratidis, H. (2019). MITIGATE: A dynamic supply chain cyber risk assessment methodology. *Journal of Transportation Security*, *12*(1–2), 1–35. https://doi.org/10.1007/s12198-018-0195-z

Söner, Ö., Kayisoglu, G., Bolat, P., & Tam, K. (2023). Cybersecurity risk assessment of VDR. *Journal of Navigation*, *76*(1), 20–37. https://doi.org/10.1017/S0373463322000595

Svilicic, B., Kamahara, J., Rooks, M., & Yano, Y. (2019). Maritime Cyber Risk Management: An Experimental Ship Assessment. *Journal of Navigation*, *72*(5), 1108–1120. https://doi.org/10.1017/S0373463318001157

Svilicic, B., Rudan, I., Frančić, V., & Doričić, M. (2019). Shipboard ECDIS Cyber Security: Third-Party Component Threats. *Pomorstvo*, *33*(2), 176–180. https://doi.org/10.31217/p.33.2.7

Svilicic, Rudan, Jugović, & Zec. (2019). A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. *Journal of Marine Science and Engineering*, *7*(10), 364. https://doi.org/10.3390/jmse7100364

Tabak, N. (2021, June 15). *HMM targeted in cyberattack*. https://www.freightwaves.com/news/hmm-targeted-in-cyberattack

Tam, K., & Jones, K. (2018). Cyber-Risk Assessment for Autonomous Ships. *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1–8. https://doi.org/10.1109/CyberSecPODS.2018.8560690

Tam, K., & Jones, K. (2019). MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, *18*(1), 129–163. https://doi.org/10.1007/s13437-019-00162-2

Torbati, Y., & Saul, J. (2012, October 22). *Iran's top cargo shipping line says sanctions damage mounting*. https://www.reuters.com/article/us-iran-sanctions-shipping-idUSBRE89L10X20121022/

Turner, A., McCombie, S. J., & Uhlmann, A. J. (2024). The Impacts of Cyber Threat in the Maritime Ecosystem. *Frontiers in Computer Science*, *6*. https://doi.org/10.3389/fcomp.2024.1378160

Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T.-E., & Nazir, S. (2022). Cyber security risk assessment in autonomous shipping. *Maritime Economics & Logistics*, *24*(2), 208–227. https://doi.org/10.1057/s41278-022-00214-0

White House. (2020). *National Maritime Cybersecurity Plan to The National Strategy for Maritime Security*. White House.

Whitley, A., & Doan, L. (2023, November 12). *Australia Cyberattack Leaves 30,000 Containers Stuck at Ports*. https://www.bloomberg.com/news/articles/2023-11-12/australian-port-operations-slowly-resume-after-cyberattack-on-dp#xj4y7vzkg

Wienberg, C. (2017, August 16). Maersk Says June Cyberattack Will Cost It up to $300 Million. *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2017-08-16/maersk-misses-estimates-as-cyberattack-set-to-hurt-third-quarter

Yoo, Y., & Park, H.-S. (2021). Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans in Consideration of Digitalized Ship. *Journal of Marine Science and Engineering*, *9*(6), 565. https://doi.org/10.3390/jmse9060565

Yungratog, S., Goerlandt, F., Punurai, W., & Thammaboosadee, S. (2022). A Conceptual Framework for Assessing Risks for Data Protection Impact Assessment Process in Maritime Industries. *2022 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 1083–1087. https://doi.org/10.1109/IEEM55944.2022.9989595

Declaration of interests

☒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.

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