Received: 18.11.2025
Accepted: 01.03.2026
Published Online:29.06.2026
DOI: 10.18613/deudfd.1826081
Research Article

Dokuz Eylül University
Maritime Faculty Journal
Vol:18 Issue:1 Year:2026 pp:1-33
E-ISSN: 2458-9942

NAVIGATING CYBER THREATS: FACTORS SHAPING LNG VESSEL DECK OFFICERS' PERCEPTION OF CYBER RISKS

OZAN BATMAZ[1]
BARIŞ KULEYİN[2]
NERGİS ÖZİSPA[3]

ABSTRACT

Considering the hazards posed by Liquefied Natural Gas (LNG) vessels, their operations on critical infrastructure, and integrated digital systems, a successful cyber-attack against LNG ships could have severe consequences. The cyber risk perception of deck officers will influence decision-making mechanisms in the face of potential threats. Therefore, identifying the factors affecting the cyber risk perception of deck officers working on LNG vessels will be beneficial in shaping their perception and strengthening decision-making mechanisms against potential cyber threats. The purpose of this research is to identify the factors influencing the cyber risk perception of deck officers working on LNG vessels. To achieve this goal, semi-structured face-to-face interview questions were directed to voluntary experts involved in LNG vessel operations. The obtained data were coded using a constant comparative analysis method. The contextual model developed within the results of the research includes factors such as "technical support", "software measures", "company's approach to cybersecurity", "company-ship communication", "company training", "insufficient knowledge", "lack of awareness of danger", "excessive optimistic approach", "onboard discipline", and "past incidents".

Keywords: *Cyber Security; Cyber Threats; Cyber Risk Perception; Maritime Transportation; LNG*

1 Lecturer, Muğla Sıtkı Koçman University, Datça Kazım Yılmaz Vocational School, Department of Transportation Services, Marina and Yacht Management Program, Muğla, Türkiye, 0000-0002-3599-3140.

2 Assoc. Prof. Dr., Dokuz Eylül University, Maritime Faculty, Department of Maritime Transportation and Management Engineering, Navigation Division, İzmir, Türkiye, 0000-0001-6485-5591

3 Corresponding Author: Assist. Prof. Dr., Mersin University, Maritime Faculty, Department of Maritime Business Administration, Mersin, Türkiye. 0000-0002-2467-5286

SİBER TEHDİTLERDE SEYİR: LNG GEMİLERİNDEKİ GÜVERTE ZABİTLERİNİN SİBER RİSK ALGISINI ŞEKİLLENDİREN FAKTÖRLER

ÖZ

Sıvılaştırılmış Doğal Gaz (LNG) tankerlerinin oluşturduğu tehlikeler, kritik altyapı üzerindeki operasyonları ve entegre dijital sistemleri göz önünde bulundurulduğunda, LNG gemilerine yönelik başarılı bir siber saldırı ciddi sonuçlara yol açabilir. Güverte zabitlerinin siber risk algısı, olası tehditler karşısında karar alma mekanizmalarını etkileyecektir. Bu nedenle, LNG gemilerinde çalışan güverte zabitlerinin siber risk algısını etkileyen faktörlerin belirlenmesi, algılarını şekillendirmede ve olası siber tehditlere karşı karar alma mekanizmalarını güçlendirmede faydalı olacaktır. Bu araştırmanın amacı, LNG gemilerinde çalışan güverte zabitlerinin siber risk algısını etkileyen faktörleri belirlemektir. Bu hedefe ulaşmak için, LNG gemi operasyonlarında görev alan gönüllü uzmanlara yarı yapılandırılmış yüz yüze görüşme soruları yöneltilmiştir. Elde edilen veriler, sürekli karşılaştırmalı analiz yöntemi kullanılarak kodlanmıştır. Araştırma sonucunda geliştirilen bağlamsal modelde; "teknik destek", "yazılım önlemleri", "şirketin siber güvenliğe yaklaşımı", "şirket-gemi iletişimi", "şirket eğitimi", "yetersiz bilgi", "tehlike farkındalığının eksikliği", "aşırı iyimser yaklaşım", "gemi içi disiplin" ve "geçmiş olaylar" gibi faktörler ortaya çıkmıştır.

Anahtar Kelimeler: *Siber Güvenlik; Siber Tehditler; Siber Risk Algısı; Deniz Taşımacılığı; LNG*

1. INTRODUCTION

Initially emerging in Germany and creating global awareness by highlighting the transformation potential of digital technologies in the manufacturing sector (Caruso, 2018), Industry 4.0 has been driving significant transformations across various sectors. It is a process in which the tools, operations, and methods of the physical world are integrated with digital technologies to create intelligent and interconnected production systems (Skobelev et al., 2017). More broadly, Industry 4.0 represents a paradigm where machines and digital systems are interconnected, enabling real-time monitoring and automation through smart systems that integrate technologies such as the Internet of Things (IoT), big data analytics, and artificial intelligence (AI), making production processes more efficient, flexible, and innovative (Butt, 2020). While the adoption of these technologies enhances operational efficiency and safety, it also exposes shipboard systems to new cyber-related vulnerabilities. Deck officers' awareness of these vulnerabilities is a key factor influencing the perception and management of cyber risks during routine onboard operations.

Due to the continuous evolution and transformation of cyber threats, organizations, despite having limited resources, must minimize their attack surfaces and enhance their security postures. Consequently, security has become a risk-based activity where operational and economic costs define risk tolerance thresholds, requiring the full integration of an organization's mission and business processes with cybersecurity measures (Nurse et al., 2017).

Cybersecurity encompasses technologies and processes designed to protect computers, networks, programs, and data from attacks, damage, or unauthorized access (Kaur et al., 2023). In the digital age, everything is increasingly interconnected as part of the accelerating digital transformation of modern societies. This transformation affects various sectors, including education, healthcare, economy, and energy (Bekkali et al., 2023). The maritime sector is no exception to this interconnected transformation process. Particularly, Information Technology (IT) and Operational Technology (OT) systems have been undergoing constant changes and evolution. These changes manifest in hardware and software modifications, the introduction of personnel with different skill sets, alterations in system architectures, shifts in supply chain structures, and adaptations in physical and technical access control measures (Chatziamanetoglou and Rantos, 2023).

In the current era of Industry 4.0, manufacturers have begun incorporating modern technologies such as IoT or Industrial IoT, AI, and Machine Learning (ML) into their operations, alongside cloud computing systems (Młody et al., 2023). Due to the rising popularity of IoT and the growing reliance on digitalization, various cybersecurity incidents and attacks have increased rapidly in recent years (Sarker, 2021). Internet security technology is one of the fastest-growing market trends. Big data and cloud computing technologies assist firms in identifying and assessing risks while simultaneously contributing to market growth (Wang et al., 2022). Effective cyber-attack detection and response help minimize economic losses, support sustainability, reduce electronic waste, maintain trust, enhance energy efficiency, promote digital transformation, ensure supply chain resilience, and prevent potential environmental damage (Albakri et al., 2023). Thus, this study is situated within the context of the increasing adoption of Industry 4.0 driven technologies in the maritime industry, particularly on LNG vessels. Accordingly, this study seeks to understand the factors shaping cyber risk perception among deck officers working on LNG vessels. Specifically, it considers how the increasing integration of Industry 4.0 driven technologies in maritime operations and deck officers' cybersecurity awareness influence their perceptions of cyber-related risks.

In the literature section of this study, the concepts of cyber-attack and cyber security will be introduced and the importance of these two concepts in the maritime industry will be discussed. Then, in the methodology section, information about the procedures for conducting Semi-Structured Face-to-Face Interviews and the experts included in the study will be given and the findings of the study will be presented. The discussion and findings sections of the study will be followed by recommendations for future studies and limitations of the study.

2. CYBERSECURITY IN MARITIME LITERATURE

2.1. Cyber-Attacks in Maritime Industry

Cyber-attacks are categorized into two types as syntactic attacks and semantic attacks (Odeh et al., 2020). Syntactic attacks involve actions that damage computer networks or software through methods such as worms, viruses, spyware, or adware (Mohan et al., 2018). In contrast, semantic attacks are a type of cyber threat designed to deceive the target individual by using techniques such as phishing or pop-up advertisements (Odeh et al., 2020). Phishing attacks are a type of cyber threat where attackers employ various methods, such as email, fake links, or phone calls, to obtain sensitive user information such as usernames, passwords, and other personal data (Astya, 2016). Phishing emails typically appear to be sent by legitimate institutions or familiar individuals, attempting to trick the recipient into clicking on a link that redirects them to a counterfeit website that appears trustworthy (Abroshan et al., 2021). Distributed Denial-of-Service (DDoS) attacks on the other hand, overwhelm target systems, such as servers, with excessive requests, leading to system slowdowns or crashes. This type of cyber-attack poses significant risks, especially in the context of the Internet of Things (IoT) (Ibrahim et al., 2022). Port scanning is a method used to identify which ports on devices within a network are open, allowing attackers to detect potential vulnerabilities. However, this method is not solely used for malicious purposes; network administrators also utilize port scanning to detect and address security weaknesses (Paolucci et al., 2019).

Malicious software, also known as malware, infiltrates digital systems through network connections or hidden within files. It is designed to execute predetermined objectives, such as capturing encrypted files or deleting data (Herr, 2014). Ransomware is divided into crypto ransomware and locker ransomware. Crypto ransomware encrypts files, leaving victims helpless without the decryption key, while locker ransomware locks or disables specific services on the victim's machine. Attackers demand ransom in exchange for returning the seized data or reactivating the disabled systems (Alqahtani and Sheldon, 2022). The Trojan virus disguises malicious software as a regular file. It aims to take control of a

user's computer, steal data, and introduce additional malware into the target system (Norton, 2018).

Similarly, a supply chain attack refers to a deliberate action or assault aimed at compromising the processes, procedures, and delivery of products, information flows, and services within a supply chain consisting of organizations, suppliers, consumers, and partners (Yeboah-Ofori and Islam, 2019). Social engineering is defined as a method that exploits human nature's vulnerabilities and takes advantage of people's naivety (Aldawood and Skinner, 2019). A successful social engineer can impersonate others, manipulate individuals, and gain unauthorized access to personal or system information (Smith et al., 2013).

When it comes to the maritime industry, it employs IoT tools to maintain a competitive advantage and meet the increasing demands of the global economy. IoT devices in the maritime sector have found applications in various segments, such as operational equipment and sensors monitoring environmental conditions. These devices are widely used in ships and port operations to reduce the risk of critical component failures, enhance operational efficiency, and provide real-time data on cargo temperature and gas emissions. While these advancements help optimize operations, reduce maintenance costs, and improve overall ecosystem security, the industry's growing reliance on data and complex network connections exposes new vulnerabilities that cyber attackers may exploit (Sahay et al., 2019).

Several maritime organizations and ports, including the UN shipping agency IMO, German cruise operator AIDA, Norwegian cruise operator Hurtigruten, Port of Kennewick, US transportation and shipping company Matson, British ferry firm Red Funnel, French container carrier CMA CGM, Greek shipping company Diana Shipping, Transport Malta, cruise operator Carnival Corporation and plc, Norwegian shipbuilder Vard, shipping company MSC, British marine services provider James Fisher and Sons, COSCO Shipping Lines, Port of San Diego, Port of Barcelona, British ship broker Clarksons, Port of Antwerp, and Maersk, have been subjected to cyber-attacks (Meland et al., 2021).

2.2. Cybersecurity in the Maritime Industry

Maritime cybersecurity, particularly concerning integrity and accessibility, is an integral part of maritime security, focusing on the protection of all aspects of maritime cyber systems against cyber threats. Additionally, it involves mitigating the consequences of cyberattacks targeting maritime operations. Therefore, maritime cybersecurity tools comprise not only technological elements but also information and human factors (Hareide et al., 2018).

Maritime IoT devices not only inherit common security threats from general IoT applications but also face additional cybersecurity challenges due to factors such as long-distance communication support and low-bandwidth connectivity. Consequently, securing IoT in the maritime industry is a major concern for the sustainability and security of the sector, as successful cyberattacks could harm national security and impact the global economy (Mudra et al., 2023).

Another critical component requiring cybersecurity in the digitalized world is cyber-physical systems. A cyber-physical system (CPS) consists of sensors used to detect changes in the physical environment, actuators that control or influence these changes, and computing and control units that analyze these changes, make decisions, and respond automatically (Kampourakis et al., 2023). In the maritime industry, cyber-physical systems integrate communication technologies, operational technologies, and human operators responsible for managing, controlling, and operating these systems. In information and operational technology systems used for performance and financial functions, human involvement exists in the form of physical or remote operators (Progoulakis et al., 2021). The issue of cybersecurity in the maritime sector is addressed under two main headings as human factors and security against cyber threats to ships.

2.3. The Human Factor in Cybersecurity

Risk is an individual's subjective state concerning uncertainty (Meng et al., 2021). Individuals use their subjective perceptions to construct their reality and assess risks (Larsen and Lund, 2021). Risk perception is a complex cognitive and psychological process that influences personal evaluations, attitudes toward risks, the likelihood of engaging in specific behaviors, and decision-making processes in uncertain situations (Voinson et al., 2015). As a multidisciplinary concept, risk perception and risk analysis are present in fields such as engineering, psychology, sociology, culture, and cognitive sciences (Larsen and Lund, 2021). While expert analysts utilize risk assessment to evaluate hazards, most people develop an intuitive risk perception by following global events, accidents, and threats through media or their surroundings (Slovic, 2016). The way individuals perceive risk, combined with their information-seeking processes and interpersonal communication, can shape their decision-making mechanisms in maritime industry (Meng et al., 2021).

It is crucial for companies in the maritime sector to be aware of existing risks and take preventive measures to mitigate them. These measures include developing cybersecurity protocols and procedures, conducting regular system maintenance and testing, training personnel, and ensuring compliance with legal regulations and standards (Barnett et al., 2023). This is particularly important because a successful cyberattack

can severely impact assets, the environment, and human safety (Longo et al., 2023).

Since technology may fail due to cyber threats, a human will ultimately be expected to find a solution to the problem. Therefore, when considering maritime cyber threats, the human element must also be taken into account (Lutzhoft et al., 2019). A significant number of cybersecurity incidents stem from human factors. In cyberattacks such as phishing or social engineering, as well as in cases where malicious software is unknowingly downloaded, human negligence plays a crucial role. Additionally, the lack of adequate preparation and competence when facing a cyberattack further exacerbates the situation (Ahvenjärvi et al., 2019).

2.4. Cyber Threats Against Ships

As the maritime industry undergoes the Industry 4.0 revolution, ships and maritime infrastructure are becoming increasingly interconnected, exposing the sector to new risks such as a higher potential for cyberattacks (Bolbot et al., 2022). The industry relies on communication and information exchange among various heterogeneous systems and devices (Penera and Chasaki, 2015). The concept of interconnection not only enables bidirectional data flow among production resources but also requires a sufficient level of abstraction for synergistic and intelligent interaction to contribute effectively to value creation (Aiello et al., 2020). Integrating detection and communication devices into a complex system enhances monitoring and communication capabilities, linking the physical dimension with the virtual world of data processing. To achieve this, ship information systems must be properly designed and deployed onboard (Aiello et al., 2020).

Advancements in ship design and functionality through new technologies improve operational efficiency, safety levels, and service quality for customers (Ben Farah et al., 2022). These technological developments, including GPS, Automatic Identification Systems (AIS), and Electronic Chart Display and Information Systems (ECDIS), provide crew members with a more comprehensive real-time view of onboard and external conditions. However, while modern ships require fewer crew members for management, increased reliance on technology heightens their presence in cyberspace, making them more susceptible to cyberattacks and introducing new attack vectors (Tam et al., 2012).

Ships are equipped with mandatory data collection and transmission devices such as AIS, Voyage Data Recorders (VDR), and Automatic Radar Plotting Aids (ARPA), generating vast amounts of data from various sources, including traffic, cargo, weather, and machinery data (Aiello et

al., 2020). These data are utilized by both IT and OT Systems. IT systems store and process information related to crew members, ship policies, certificates, and compliance documents, whereas OT systems control ship operations, including thruster direction, rudder angle, cargo handling, ballast water management, power distribution, and navigation aids (Kanwal et al., 2022). However, this technological growth increases cyber risks, leaving navigation and control systems vulnerable to cyberattacks (Hemminghaus et al., 2021).

Modern cyberattacks are becoming more discreet and harder to detect, leading to prolonged exploitation of compromised ships, causing operational disruptions, financial losses, reputational damage, environmental harm, legal issues, and high response costs (Tam et al., 2012). The latest developments in the maritime industry include the research and development of sophisticated, smart ships with advanced autonomy. However, as autonomy and interconnectivity increase, vessels become more susceptible to cyber threats that could result in financial losses, environmental pollution, and safety incidents (Bolbot et al., 2020).

False Data Injection (FDI) attacks are cyber threats that manipulate measurement data to affect the state estimation of power grids (Liu et al., 2011). Direct Current (DC) microgrids are increasingly incorporating complex software-based controllers and communication networks, evolving into cyber-physical systems with intricate interactions between physical and software processes, making them vulnerable to cyberattacks (Beg et al., 2017). Modern ship power systems, equipped with advanced cyber infrastructures, are at a higher risk of cyberattacks and thus require urgent maintenance. Specifically, false data injection attacks can interfere with measurement devices, distort state estimation, or directly target central control systems (Kushal et al., 2018). False data injection attacks on shipboard DC microgrids may lead to the prioritized activation of a large load during port maneuvers, resulting in system failures and severe maritime collisions (Zeng et al., 2022). The key to preventing false data injection attacks lies in detecting false data and implementing countermeasures (Zeng et al., 2022).

Voyage Data Recorders (VDR), often referred to as the "black boxes" of the maritime industry, collect and store crucial data from key sensors and locations around the vessel, playing a vital role in accident or incident investigations (Zong and Zhao, 2018). Most VDRs consist of a core module that collects information from sensors and bridge equipment and stores it in internal hard drives, two external storage units (one fixed and one float-free) and a bridge interface with a Graphical User Interface (GUI) that allows crew members to monitor the status of the VDR (Hopcraft et al., 2023). The VDR core unit typically includes a standard interface

(Universal Serial Bus – USB) for data uploading/downloading, a dedicated computing device that runs the VDR software, and an input/output interface (Ethernet or serial) for receiving data from sensors and sending logs to storage. Additionally, the core unit contains two mirrored hard drives designed to ensure redundancy in case of drive failure (Piccinelli and Gubian, 2013). The use of common interfaces such as USB for software updates and data downloads introduces multiple security vulnerabilities for the VDR. To mitigate these vulnerabilities, proprietary interfaces or software should be employed, and access to the device should be limited to authorized personnel with direct physical access and the correct connection devices (Hopcraft et al., 2023).

Traditionally, core navigational responsibilities such as ship handling, collision avoidance, and position tracking were manually performed by the officer on watch. However, with modern technology, officers now operate more like system operators, monitoring the ship's position and course primarily through an Electronic Chart Display and Information System (ECDIS) integrated with the Global Navigation Satellite System (GNSS), thereby allowing them to perform additional duties (Erstad et al., 2021). A malicious software attack on a vessel's ECDIS system could pose significant risks, affecting not only commercial vessels but also all types of ships (Androjna and Perkovič, 2021).

The maritime sector possesses its own open-source information, which can be exploited by malicious actors targeting computer systems and human elements (Fitton et al., 2015). For instance, the Automatic Identification System (AIS) performs functions such as ship identification, target tracking, information exchange, and situational awareness enhancement by providing supplementary data (Oruc et al., 2022). A cyber-attacker could access an AIS receiver through the appropriate radio channel and use a Frame Check Sequence (FCS) similar to that of an AIS decoder, injecting false data that could lead to ship collisions (Balduzzi et al., 2014).

Autonomous ships, which integrate advanced artificial intelligence technologies, big data, and sensors, are expected to reduce operational costs and enhance maritime safety. However, due to the high level of ship-to-shore connectivity required for their operation and land-based management systems, these vessels remain highly susceptible to cyber threats (Zagan et al., 2022). Ensuring the security of autonomous vessels necessitates the implementation of multiple positioning systems. Commonly used systems such as GPS, Radar, LiDAR, AIS, and ECDIS provide real-time data on ship position, cargo information, and navigation details, playing a critical role in ensuring the safety of the vessel, its cargo, and surrounding ships and personnel (Silverajan et al., 2018). These

systems facilitate a continuous flow of data to autonomous ships, enabling them to perform functions such as situational recognition and perception, judgment, action, and control through artificial intelligence, while their operational outcomes are monitored by shore-based control centers or onboard crew (Dugan et al., 2023). Judgment technologies utilize collected and predicted data from vision systems, allowing autonomous ships to navigate, berth, and anchor automatically, determine safe and cost-effective routes based on maritime conditions, and predict and respond to potential failures (Yoo and Jo, 2023). Hence, if a cyber-attacker targets vulnerable points during the artificial intelligence learning phase, the autonomous vessel may make incorrect decisions due to erroneous learning, leading to severe consequences (Alop, 2019). Accordingly, this study aimed to determine the factors affecting the cyber risk perception of deck officers. LNG vessels, which are in the high risk group due to the nature of the product group they are related to, were determined as a sample. Detailed information on the methodology used in the study is provided in the next section.

3. METHODOLOGY

3.1. Research Design

This study adopts an exploratory qualitative research design to investigate the factors shaping the cyber risk perception of deck officers serving on LNG vessels. Exploratory qualitative designs are particularly suitable for research areas where existing theoretical knowledge is limited and require an in-depth understanding of the phenomenon under investigation based on participants' experiences and interpretations (Larsen et al., 2022). Given that maritime cyber threats are a relatively new and complex field of study and considering the limited empirical evidence focusing on LNG vessels, a qualitative approach was deemed appropriate to capture the nuanced perceptions and contextual factors influencing cyber risk perception.

3.2. Semi-Structured Face-to-Face Interview Phase

In this research, 18 semi-structured face-to-face interview questions from Larsen et al. (2022) were used, with permission from the authors, to analyze the factors influencing the cyber risk perceptions of deck officers working on LNG vessels. Before conducting the interviews, appointments were scheduled with participants, ensuring their availability in terms of time and location. The interviews were conducted both face-to-face and online, during which the 18 pre-prepared semi-structured questions were asked. In cases where responses were unclear or off-topic, the interviewer provided additional explanations without directly influencing or leading the participant’s opinions, ensuring that discussions remained within the

research scope. Each interview conducted with an expert lasted on average between 1 to 1.5 hours. At the end of the interviews, the necessary data was successfully collected.

3.3. Expert Group Selection

To obtain the necessary data for this study, expert interviews were conducted with masters, chief officers, and watchkeeping officers working on LNG vessels. Considering that the frequency of IT and OT system usage varies depending on crew members' roles, special attention was given to forming an expert group with diverse qualifications and positions. For instance, chief officers tend to use operational technology systems more frequently, while masters rely more on communication technologies.

3.3.1. Sampling Strategy and Participant Recruitment

To include participants with direct operational experience and expertise in LNG, a purposive sampling strategy was employed in the study. Additionally, based on insights from the literature review, demographic factors such as age were identified as influential in the adaptation process to technological advancements (Magsamen-Conrad and Dillon 2020; Onyeaka et al., 2021). Therefore, purposive sampling strategy aimed to increase sample heterogeneity by including participants from diverse professional roles, experience levels, ages, and genders, thereby allowing for the exploration of different perspectives on cyber risk perception. Participation criteria included actively working as deck officers (Captain, Chief Officer, or Watch Officer) on LNG vessels and regularly interacting with the ship's IT and OT systems. Participants were selected through professional networks, industry connections, and peer recommendations within the maritime sector. Participation was entirely voluntary, and interviews were conducted only with those who agreed to participate. Considering these criteria, the expert group was composed of seven LNG vessel personnel with varying qualifications, positions, maritime experience, gender, and age.

Table 1: Expert Group

Number	Position	Total Experience Onboard	LNG Experience	Gender	Age
E1	Master	17 Years	17 Years	Male	38
E2	Master	13 Years	12 Years	Male	48
E3	Master	10 Years	1 Years	Male	38
E4	Master	17 Years	2 Years	Male	43

E5	Chf.Off.	6 Years	6 Month	Male	30
E6	2nd.Off	3 Month	3 Month	Female	25
E7	2nd.Off	1 Years	1 Years	Female	25

3.3.2. Sample Size and Theoretical Saturation

The final sample consisted of seven deck officers working on LNG vessels. While this number may seem limited, it is consistent with qualitative research practices in highly specialized and difficult-to-access professional fields such as LNG transportation. Due to the limited number of LNG vessels worldwide and their intensive operational schedules, access to suitable participants was restricted. A review of the existing literature shows that the sample size used in qualitative studies employing officers working on LNG vessels ranges from 5 to 10 people (Hatmi, et al., 2024; Kustanto, 2023). More importantly, data collection was guided by the principle of theoretical saturation. Interviews and data analysis were conducted simultaneously using a continuous comparative analysis approach. After the seventh interview, no new themes, categories, or conceptual insights emerged from the data. At this point, theoretical saturation was considered to have been reached, and therefore data collection was terminated.

3.4. Constant Comparative Analysis Method

In this study, qualitative data obtained from semi-structured interviews were analyzed using the Continuous Comparative Analysis (CCA) method. Although initially developed within the grounded theory methodology, CCA is widely used as a qualitative data analysis technique in exploratory studies (Leong et al., 2010). It is employed to understand the complexity of qualitative research, enabling researchers to simultaneously analyze and code raw data, such as observations or interview transcripts, to develop theories (Kolb, 2012). This method is based on systematic comparison and involves forming categories, defining their boundaries, assigning data segments to categories, summarizing each category's content, identifying contradictory evidence, and refining conceptual distinctions to develop models (Boeije, 2002).

Interview transcripts were iteratively coded, and data were continuously compared across interviews to identify similarities and differences in this study. The resulting codes were grouped into sub-themes and then organized under broader themes. This iterative process facilitated the refinement of categories and ultimately led to the development of the contextual model presented in Figure 1.

In this study, data obtained through semi-structured interviews with voluntary participants were analyzed using the constant comparative analysis method, leading to the development of a contextual model. After each interview, responses to the semi-structured questions were analyzed, and the coding process began. Initial data analysis guided the formation of subcategories, which were expanded and categorized under main themes as new interviews provided additional insights. Following the principles of constant comparative analysis, the coding process proceeded concurrently with the interview phase, ensuring continuous refinement. Once all interviews were completed, the final dataset was analyzed and coded, resulting in the creation of a contextual model.

3.5. Trustworthiness of the Study

To ensure the rigor of the qualitative research process, this study followed widely accepted criteria for trustworthiness, namely credibility, transferability, dependability, and confirmability. Credibility was addressed by using semi-structured interviews that allowed participants to describe their experiences and viewpoints in their own terms. All interviews were conducted by the same researcher and followed a consistent interview guide, which helped maintain coherence across the data collection process. Throughout the analysis, the researcher repeatedly returned to the interview data to check whether the emerging themes accurately reflected participants' accounts. Transferability was supported by providing detailed information about the research context, the operational environment of LNG vessels, and the professional characteristics of the participants. By describing these elements in detail, the study allows readers to evaluate the extent to which the findings may be applicable to similar maritime settings. To enhance dependability, data collection and analysis were carried out in a systematic and transparent manner. Interview procedures and analytical steps were clearly defined, and the constant comparative analysis approach enabled the consistent treatment of data across interviews. Confirmability was strengthened by grounding interpretations directly in the interview data. The findings were supported with verbatim quotations from participants, which helped ensure that the analysis remained closely connected to the participants' perspectives rather than the researcher's assumptions.

4. FINDINGS

The findings of the study, which investigates the factors influencing the cyber risk perceptions of deck officers working on LNG vessels, are presented in the contextual model in Figure 1. The key factors affecting these perceptions include third-party measures, organizational approaches, onboard discipline, insufficient knowledge, and previous cyber incidents.



Figure 1: Contextual Model of Factors Influencing Cyber Risk Perceptions Among Deck Officers Working on LNG Vessels

4.1. Third-Party Measures

The findings derived from semi-structured face-to-face interviews indicate that one of the significant factors affecting the cyber risk perception of personnel working on LNG vessels is third-party security measures, such as IT departments, firewalls, antivirus software, and encryption systems. Participants reported relying heavily on software solutions and IT departments for the management of cyber risks, which they viewed as beyond their professional expertise. It was noted that in some organizations, in-house IT teams provide these third-party security measures, while in others, external technical teams are responsible for implementing them.

4.1.1. Technical Support

According to the findings from semi-structured face-to-face interviews, another important factor affecting the cyber risk perception of personnel aboard LNG vessels is third-party security measures, including IT departments, firewalls, antivirus software, and encryption systems. The participants expressed significant trust in software solutions and IT departments for managing cyber risks, considering them to be outside their

professional domain. These measures are provided by in-house IT teams in some companies, while in others, external technical teams handle them. One of the interview outputs that led to this finding is included below.

"No programs can be installed on our computers from outside. For example, if I wanted to install a program like 'Port to Port' on a computer, the system doesn't allow it. Only IT personnel are authorized to install programs. If any other program is installed, an automatic email is sent to the IT department saying, 'A new program has been installed on this computer aboard the ship.' And the program is removed from the computer."

4.1.2. Software Measures

The findings obtained from semi-structured face-to-face interviews reveal that one of the major factors influencing the cyber risk perceptions of personnel aboard LNG vessels is the reliance on external third-party security measures, including IT departments, firewalls, antivirus software, and encryption systems. Participants emphasized the importance of software solutions and IT departments in managing cyber risks, acknowledging that these issues are often beyond their areas of expertise. The responsibility for these measures is either with in-house IT teams or external technical teams, depending on the organization.

4.2. Approach of the Organization to Cybersecurity

The findings of the interviews suggest that the cyber risk perception of deck officers working on LNG vessels aligns with the organization's approach to cybersecurity. In companies that focus more on cybersecurity, have clear company procedures in place, provide pre-voyage training on the subject, and communicate information digitally to the vessels, officers were found to be more aware of cyber risks and behaved more carefully and responsibly when using onboard digital systems. On the other hand, officers working in companies that did not pay sufficient attention to cybersecurity were observed to be more flexible regarding cyber risks and less prepared for such risks.

4.2.1. Organization's Strict Approach

Some experts reported that their organizations placed significant importance on cybersecurity, allocating a specific section for cybersecurity in the PMS system on their vessels, issuing circulars regarding cybersecurity, conducting both pre-voyage and onboard training, and notifying the vessels about cyber incidents at sea to prevent similar occurrences. These experts were observed to act more carefully and be more knowledgeable about cyber risks.

4.2.2. Organization's Flexible Approach

Some experts stated that their organizations did not give sufficient attention to cybersecurity and, although they suggested measures to mitigate cyber risks, the company viewed these suggestions as additional costs. This attitude of the company towards cybersecurity was reflected in the behavior of the crew onboard. These experts observed that the personnel had lower awareness of cyber risks and acted less cautiously. One of the interview outputs that led to this finding is included below.

"Companies seem to view spending money and time on this matter as a luxury. We can't convince the shipowner. When we suggest something like, 'We need to do this for cybersecurity,' we often get responses like, 'Is this really necessary?' Only after something big happens, like what happened with Maersk, do we start taking preventive measures. This is how things work in the maritime industry as well. Something happens, and then we start taking precautions."

4.2.3. Communication Between Organization and Vessel

Experts shared that in some organizations, incidents occurring in external institutions or aboard other vessels were reported to the vessel via phone, with instructions to take preventive measures to avoid similar situations. These companies were found to limit their communication on cybersecurity to verbal notifications, without using emails, circulars, or any other forms of written communication. This approach was found to be reflected in the crew's behavior regarding cybersecurity, as they acted more carelessly and lacked awareness. On the other hand, experts from organizations that provided written instructions on necessary cybersecurity measures, issued regular circulars, supported and followed up on cybersecurity training in writing, and had a dedicated section for cybersecurity in the PMS system observed that the crew on those vessels acted more cautiously and followed company procedures to implement necessary measures. Examples of the interview outputs that led to this finding is included below.

"No emails have been received for cyber-attack measures so far. There have only been verbal warnings."

"We are still a new company. However, the company absolutely prioritizes cybersecurity. Especially when they hear about a cyber incident, they are so attentive and aware of the issue that they will call the ship no matter what time it is and say, 'Look, such an incident occurred, be careful.' Our company is very sensitive about this."

4.2.4. Organization's Training Programs

The cybersecurity training provided by organizations both before and during the voyage emerged as one of the factors influencing deck officers' cyber risk perception. Some experts mentioned that their organizations did not organize any cybersecurity training, and when human error or negligence related to cybersecurity was observed onboard, the crew was simply warned by their superiors. However, the personnel were not provided with more in-depth information beyond these warnings. These experts further indicated that, as they could not observe the crew continuously, such actions occurred outside of their supervision, and the vessel's systems were at risk from cyber threats. On the other hand, experts working for organizations that organized both pre-voyage and onboard cybersecurity training reported greater awareness among themselves and their personnel. The interviews with these experts revealed that they and the crew on their vessels were more aware of cyber risks and that the pre-voyage and onboard training had positively influenced their behavior when using IT and OT systems, leading to more cautious and responsible actions. One of the interview outputs that led to this finding is included below.

"The ship, although built in 2021, has systems that are not found on most commercial vessels. Since I have received training on these systems, I am able to understand the majority of them."

"Our company provides us with training on this matter before joining the ship. They are very sensitive about it. This, of course, affects the behavior of the staff. We have an IT department, and we seek their help when necessary. Actually, all companies should provide this kind of training, but we know that not every company does."

4.3. Insufficient Knowledge

The semi-structured interviews revealed that some experts lacked sufficient knowledge regarding the diversity and complexity of cyber threats arising in parallel with the rapid technological changes in the maritime sector. While some experts discussed various cyber threats that could target the ship's IT and OT systems, others limited their understanding of cyber threats to the term "virus." These experts believed that many systems were secure from cyber threats or that the potential outcomes of a cyber incident would not lead to serious problems. This indicated that these experts exhibited overconfidence regarding cyber threats, were unaware of the potential issues that could arise from a cyber incident, and approached the topic with excessive optimism.

4.3.1. Overconfidence

It was observed during the interviews that some experts, due to their limited knowledge of cyber threats, exhibited overconfidence in their approach. These experts expressed confidence in their ability to easily resolve any encountered cyber threat, believing they could resolve any issues without affecting the ship's navigation or operations and that no significant problems would arise.

4.3.2. Unawareness of the Danger

Some experts were observed to be unaware of the potential consequences of a cyber incident or which systems onboard might be targeted by cyberattacks and the potential dangers that could result from such attacks. While some experts clearly identified potential cyber incidents, systems at risk of cyberattacks, the types of attacks that might target these systems, and the dangers resulting from such attacks, others lacked sufficient knowledge in these areas. Experts who were unaware of the types of cyber incidents that might occur onboard or the risks posed by potential cyberattacks were observed to be more flexible in their approach to cybersecurity.

4.3.3. Excessive Optimism

The findings from the research process revealed that some experts adopted an overly optimistic approach to cyber risks. These experts believed that the systems on their vessels were secure against cyber threats, that their ships would not be targeted by cyberattacks, and that the most significant issue they could face would be some viruses affecting the ship's computer systems, which they felt would not cause serious problems. During the interviews, some experts also stated that they believed cyber-attackers were more likely to target companies rather than vessels.

4.4. Onboard Discipline

Semi-structured interviews revealed that shipboard discipline is a factor influencing the cybersecurity risk perception of officers on LNG vessels. In ships where discipline is maintained regarding cybersecurity and where officers exhibiting improper or careless behavior toward cyber threats are warned and monitored by superiors, officers were observed to be more careful when using both ship devices and personal devices. In contrast, ships where this discipline and monitoring were insufficient saw officers acting with less care or only adhering to warnings while under supervision.

4.4.1. Screen Addiction

One of the notable findings in the study was the issue of screen addiction. Some experts reported that, although their companies provided limited internet access, officers often used their personal phones on the bridge to connect to the ship's wireless network. These experts expressed concern about officers spending excessive time on their personal devices during shift hours, which disrupted ship operations, and the potential risks of connecting personal devices to the ship's wireless network. They highlighted the unknown security of the apps and websites accessed by these devices, voicing their discomfort and dissatisfaction. One of the interview outputs that led to this finding is included below.

"There are restrictions on the use of phones or any personal screens during working hours. You are not supposed to use them. Of course, having internet in places like the bridge and engine room can be both good and bad. For example, there is no Wi-Fi connection for personnel use on the bridge, which was specifically removed. It used to be available, but no matter how much you warn the staff, they could still come to the bridge with their own phones and use them when you (the captain) weren't around. And as you can imagine, once they start browsing the internet and switching from one app to another, time passes, and the shift is already over. That's why we no longer allow internet on the bridge."

"There is a specific limit of internet usage for personnel on the ship. However, I get upset about internet use during working hours. Crew members should focus on the ship and their duties during their shifts. It's not appropriate for them to use their phones on the bridge. I warn them when I see it, but they do it when I'm not around."

4.4.2. Social Media Usage

One expert emphasized that while social media activity may not directly present a cyber threat, sharing ship-related information on social media could open pathways for cyber threats. They explained that posts containing ship information could be monitored from the outside, and through interconnected links and applications, more data about the ship and its crew could be accessed, potentially making the ship or company a target for cyberattacks. As a result, this expert mentioned that social media posts related to the ship were prohibited on their vessels, and crew members were expected to exercise caution in this regard. One of the interview outputs that led to this finding is included below.

"Because we are so closely connected with our phones, people now share everything, including the ship's location, on their social media accounts. The company has provided training on the potential problems this can cause. Especially when passing through pirate zones, if such

information is shared, since pirates use IT systems even more actively than we do, they can access everything from the type of ship to the personnel aboard through these shared posts. This is possible because everything is interconnected through links. For example, the attacker (hacker) sees a post on Instagram, then moves to Facebook and from Facebook to LinkedIn, following this path to get detailed information about the ship."

4.5. Experienced Cyber Incidents

The study also revealed that past cyber incidents influenced the cybersecurity risk perception of officers on LNG vessels. Although some experts stated they had not directly encountered a cyberattack, others mentioned that they learned about certain cyber incidents in the maritime sector from various sources. Some experts learned about cyber incidents aboard ships from their close circles, while others were made aware of such incidents through notifications and warnings communicated by their companies. Discussing past incidents during pre-boarding and onboard training sessions, as well as conveying case studies and preventive measures in written form to the crew, was found to be an effective method in shaping officers' cybersecurity risk perception. Examples of the interview outputs that led to this finding is included below.

"We received an email. It appeared to come from the agent. We responded to the email, transferred the money, and then tried to withdraw it, but we struggled a lot and couldn't do it. We fell into a trap with just one email. The attacker copied the agent's email exactly, the sender address was the same, and even the format was identical. All our data was copied (stolen), and the company incurred a loss of about 200,000 dollars."

"Yes, I had heard it from a friend. He was on a 170-meter, 30,000-ton chemical tanker. A virus-infected flash drive brought by an external surveyor was plugged into the ship's computer. As you know, surveyors usually bring their own flash drives, plug them into the ship's computer, do their calculations from there, and print out documents. When the virus-infected flash drive was connected to the ship's computer, there was no protection, and the virus spread through the shared network, affecting all systems. All the data and automation systems were compromised. To fix the situation, they had to bring in a technician to reset all the systems."

5. DISCUSSION

In this study, semi-structured face-to-face interviews were conducted with a group of experts to analyze the factors influencing the cybersecurity risk perception of deck officers on LNG vessels. The raw data collected were coded using the constant comparative analysis method, resulting in a contextual model. A similar study by Larsen et al. (2022) also analyzed factors affecting the cybersecurity risk perception of deck officers in

offshore operations. When comparing the contextual models of both studies, some similar findings were observed. Both studies identified factors such as “training,” “insufficient or limited information,” “overly optimistic approach,” and “reliance on technical services” as influencing the cybersecurity risk perception of officers. However, in this study, additional factors such as “company approach” and “shipboard discipline” were found to influence how cyber risks are perceived by LNG deck officers, which was attributed to interviews being conducted with experts from different companies. This study examined both strict and flexible company attitudes separately, while participants in Larsen et al.'s (2022) study expressed concerns about being continuously monitored digitally by their companies. They viewed this constant monitoring as an intrusive activity that restricted their work and management, which was included as a factor affecting the officers' cybersecurity risk perception in that study. Thus, both studies reveal that a company’s strict approach influences the cybersecurity risk perception of deck officers.

The diverse age groups and varying levels of maritime experience of the study participants provided a valuable basis for interpreting the contextual model presented in Figure 1. This participant diversity appears to have shaped how cyber risks were perceived and prioritized, reflecting differences in professional responsibilities and experience levels. More senior officers, particularly captains with extensive maritime experience, placed greater emphasis on organizational procedures, company policies, and third-party technical support, while younger and less experienced officers placed greater emphasis on individual awareness, training, and daily operational discipline.

As shown in Figure 1, the factors identified in this study interact within a broader organizational and operational context rather than functioning independently. For example, a strong organizational commitment to cybersecurity, supported by effective training programs and structured company-ship communication, appears to mitigate the negative effects of individual-level factors such as insufficient knowledge or overly optimistic attitudes. Conversely, weak organizational practices may amplify risky onboard behaviors by reinforcing low awareness and inadequate onboard discipline.

Corradini and Nardelli (2016) conducted a cybersecurity risk perception survey with 1,164 employees in a multinational electronic payment company, highlighting “risk analysis” and “training” as the most important actions for effectively preventing cybersecurity risks. This finding aligns with the training factor identified in this research. Additionally, Heering et al. (2021) systematically reviewed published maritime cybersecurity research and emphasized the role of cybersecurity

components in training programs for seafarers. They noted that while cybersecurity was not a mandatory subject in maritime training, they predicted that in the future, ship owners and companies would require seafarers to take courses or obtain certifications related to cybersecurity awareness. These measures, they suggested, would play a significant role in reducing the risks of cyber incidents that could have severe long-term consequences and costs for companies.

Bolat and Kayişoğlu (2019) investigated the factors and outcomes of cybersecurity awareness in the maritime sector by analyzing survey data from 211 maritime employees in Türkiye using Structural Equation Modeling. Similar to this study, Bolat and Kayişoğlu found that the training factor affected the cybersecurity awareness of maritime workers. However, unlike this study, their research concluded that information sharing, rules, and policies had no significant impact on cybersecurity awareness. Mittal and Ilavarasan (2019) explored the relationship between demographic differences and cybersecurity perceptions, finding that perceptions of cybersecurity varied with age, work experience, qualifications, and education. In their study, although the age factor influenced the adaptation to new systems, it did not create significant differences in approaches to cybersecurity threats and awareness. Bellekens et al. (2016) examined cyber risks and situational awareness in e-health services, finding that most participants exhibited an optimistic approach to cybersecurity risks and felt detached from these threats. Their study also revealed that most participants lacked sufficient knowledge about cybersecurity threats. Despite the different sector focus, both studies again highlighted the influence of optimistic approaches and insufficient information on cybersecurity risk perceptions.

Abroshan et al. (2021) conducted a study examining the impact of human emotions, behaviors, and demographic features on the success of phishing attacks in the maritime sector during the COVID-19 pandemic. While the study focused on emotional states and demographic factors, the authors also noted that individuals' education levels and knowledge of cybersecurity influenced the success of phishing attacks both before and during the pandemic. These findings align with the factors identified in the contextual model developed in this research.

The findings of this study are consistent with previous studies highlighting the impact of demographic characteristics on cybersecurity perceptions. In the present study, age and professional experience played a significant role in shaping cyber risk perception; more experienced officers showed greater reliance on institutional safeguards, while younger officers emphasized personal vigilance and continuous learning. This differentiation enhances the explanatory value of the contextual model

presented in Figure 1 by positioning individual perceptions within both organizational structures and career stages.

When compared with related literature, the most similar finding in this research was the importance of the training factor in influencing cybersecurity risk perception. In the face of increasing digitalization and emerging cybersecurity threats, it is believed that cybersecurity training provided both internally and externally by maritime companies, particularly those heavily utilizing IT and OT Systems, will enhance the cybersecurity risk perception of personnel.

Overall, this study contributes to the growing literature on maritime cybersecurity by providing insight into how cyber risk perception is shaped among deck officers working on LNG vessels. By integrating individual-level factors with organizational dimensions, it emphasizes that cyber risk perception is not merely a matter of technical awareness, but is also influenced by corporate practices, training policies, and the operational culture on board. The contextual model developed in this study (Figure 1) offers a structured framework that can support maritime companies in designing more effective cybersecurity strategies, training programs, and communication mechanisms tailored to different experience levels and roles on board.

6. CONCLUSION

Parallel to the rapid technological advancements in the maritime sector, cyber threats have become increasingly complex. Considering the digital systems of LNG vessels and the hazardous cargo they carry, cyberattacks targeting these vessels can pose significant security and environmental risks. This study is among one of the first known studies to examine the concept of cybersecurity, a relatively new field of study lacking sufficient examples in the literature, specifically from the LNG sector within the maritime transportation literature. Furthermore, it also qualitatively examines Turkish seafarers' perception of cyber risk. The study also suggests new operational themes, such as overreliance on technical personnel, deck officers' lack of knowledge about cyber threats, etc. The research shows that the lack of knowledge among deck officers about cyber threats makes ship operations vulnerable and weakens their ability to respond effectively to security threats. The primary causes of this deficiency are inadequate training and a lack of understanding of sector-specific threats.

The findings reveal that some deck officers exhibit overconfidence and an optimistic attitude toward cyber risks. This attitude can lead to underestimating real threats and neglecting necessary security measures. Furthermore, it is emphasized that relying solely on software measures

such as firewalls and antivirus programs is insufficient, particularly against emerging threats like malware and social engineering. It is critical for officers to develop their own perception of cyber risks in these contexts.

The study indicates that some deck officers are unaware of cyber threats, which complicates the implementation of measures to address cyber risks. In the maritime industry, cybersecurity has become as critical as physical security, and understanding risks is essential for conducting effective risk analysis. Additionally, screen addiction and the failure to maintain discipline onboard can lead officers to connect personal devices to the ship's network, allowing potential cyber threats to infiltrate the ship's systems. Therefore, raising awareness among deck officers and strengthening onboard discipline are crucial in preventing cyber incidents.

The research also shows that past cyber incidents are one of the key factors shaping deck officers' perception of cyber risks. However, many cyber incidents occurring on ships are often kept confidential due to concerns over reputation and financial loss, which hinders the learning and preventive measures within the sector. Systematic reporting of cyber incidents could guide maritime companies and contribute to new research. To this end, creating a platform that ensures confidentiality in incident reporting could provide data for more specific studies in the sector. With the increasing prevalence of autonomous vessels, the development of cyber incident reporting and detection systems will be a critical step in ensuring the future security of the maritime sector.

The study has shown that education is the primary factor influencing cyber risk perception. Rapid technological changes and increasing cyber threats in the maritime sector highlight the need for deck officers on LNG vessels to receive cybersecurity training. These officers must possess sufficient knowledge to be vigilant against cyber threats and conduct effective risk analysis while using IT and OT systems. Additionally, it was observed that maritime companies adopt different approaches to cybersecurity education, and there is no standard in this area. In an environment where training is provided, officers will be able to make more effective decisions against cyber threats, conduct accurate risk assessments, and be more mindful of their actions. It is emphasized that cybersecurity education should not be viewed as a cost but as a long-term benefit.

The study's most significant limitation is that the sample consisted of seven deck officers working on LNG vessels. However, the relatively small size of the LNG sector and the nature of the profession, particularly the presence of industry employees in international waters, made accessing the sample difficult. Despite comprising seven individuals, the sample was diversified based on their duties on the ship. This was assumed to increase

the representativeness of the sample.

This study has identified and analyzed the factors affecting the cyber risk perception of deck officers working on LNG vessels, creating a contextual model. However, it did not identify which of these factors most significantly impact cyber risk perception. Future studies can use the factors identified in this study's contextual model as a reference and conduct a study with deck officers working on tankers in general or with white-collar managers in tanker companies in Türkiye. The new survey developed using these factors could provide data, and the factors influencing cyber risk perception can be analyzed using multi-criteria decision-making techniques, such as Analytical Hierarchy Process, to identify the most prominent factors.

AUTHOR CONTRIBUTION

CONTRIBUTION RATE	EXPLANATION	CONTRIBUTORS
Idea	Pointing out the research idea or forming hypotheses	Author 1 and 2
Review of Literature	Conducting the literature review for the study	Author 1 and 3
Research Design	Forming the research design, including research methodology, deciding on scales and samples	Author 1, 2 and 3
Data Collection and Editing	Data collection, editing, and analyzing	Author 1 and 3
Findings and Discussion	Reporting and discussing the findings	Author 1, 2 and 3

Conflict of Interest

No potential conflict of interest was reported by the authors.

Financial Support

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 research.

REFERENCES

Abroshan, H., Devos, J., Poels, G. and Laermans, E. (2021). COVID-19 and phishing: effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. *IEEE Access*. 9: 121916–121929.

Ahvenjärvi, S., Czarnowski, I., Kála, J., Kyster, A., Meyer, I., Mogensen, J. and Szyman, P. (2019). Safe information exchange on board of the ship. *TransNav*. 13(1): 165–171.

Aiello, G., Giallanza, A. and Mascarella, G. (2020). Towards shipping 4.0. A preliminary gap analysis. *Procedia Manufacturing*. Elsevier B.V.: 24–29.

Albakri, A., Alabdullah, B. and Alhayan, F. (2023). Blockchain-assisted machine learning with hybrid metaheuristics-empowered cyber attack detection and classification model. *Sustainability*. 15(18): 13887.

Aldawood, H. and Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. *Future Internet.* MDPI AG.

Alop, A. (2019). the main challenges and barriers to the successful "Smart Shipping." *TransNav*. 13(3): 521–528.

Alqahtani, A. and Sheldon, F.T. (2022). A survey of crypto ransomware attack detection methodologies: an evolving outlook. *Sensors*. MDPI.

Androjna, A. and Perkovič, M. (2021). Impact of spoofing of navigation systems on maritime situational awareness. *Transactions on Maritime Science.* 10(2): 361–373.

Astya, P.N. (2016). International conference on computing, communication and automation. *Proceeding of ICCCA,* (ss. 29-30).

Balduzzi, M., Pasta, A. and Wilhoit, K. (2014). A security evaluation of AIS automated identification system. *ACM International Conference Proceeding Series.* (ss. 436 445). ACM. December 2014.

Barnett, M., Samori, I., Griffin, B., Palmer, X. and Potter, L. (2023). A commentary and exploration of maritime applications of biosecurity and cybersecurity intersections. *Proceedings of the 22nd European Conference on Cyber Warfare and Security.* 22(1).

Beg, O.A., Johnson, T.T. and Davoudi, A. (2017). Detection of False-data injection attacks in cyber-physical DC microgrids. *IEEE Transactions on Industrial Informatics.* 13(5): 2693–2703.

Bekkali, A. El, Essaaidi, M. and Boulmalf, M. (2023). A blockchain-based architecture and framework for cybersecure smart cities. *IEEE Access*. 11: 76359–76370.

Bellekens, X., Hamilton, A., Seeam, P., Nieradzinska, K., Franssen, Q. and Seeam, A. (2016). Pervasive ehealth services a security and privacy risk awareness survey. 2016 international conference on cyber situational awareness, *Data Analytics and Assessment*. Düzenleyen: CyberSA. 2016.

Ben Farah, Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I. and Bellekens, X. (2022). Cyber security in the maritime industry: a systematic survey of recent advances and future trends. *Information* (Switzerland). MDPI.

Boeije, H. (2002). a purposeful approach to the constant comparative method in the analysis of qualitative interviews. *Quality and Quantity*. 36(4): 391–409.

Bolat, P. and Kayişoğlu, G. (2019). Antecedents and consequences of cybersecurity awareness: a case study for turkish maritime sector. *Journal of Eta Maritime Science*. 7(4): 344–360.

Bolbot, V., Kulkarni, K., Brunou, P., Banda, O. V. and Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: a systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*. 39.

Bolbot, V., Theotokatos, G., Boulougouris, E. and Vassalos, D. (2020). A novel cyber risk assessment method for ship systems. *Safety Science*. 131.

Butt, J. (2020). A conceptual framework to support digital transformation in manufacturing using an integrated business process management approach. *Designs*. 4(3): 1–39.

Caruso, L. (2018). Digital innovation and the fourth industrial revolution: epochal social changes. *AI and Society.* 33(3): 379–392.

Chatziamanetoglou, D. and Rantos, K. (2023). Blockchain-Based security configuration management for ICT systems. *Electronics.* 12(8).

Corradini, I. and Nardelli, E. (2016). A case study in information security awareness improvement: a short description. *IMCIC – ICSIT.*

Dugan, S. A., Skjetne, R., Wróbel, K., Montewka, J., Gil, M. and Utne, I. B. (2023). Integration test procedures for a collision avoidance decision support system using STPA. *TransNav.* 17(2): 375–381.

Penera, E. and Chasaki, D. (2015). *Packet scheduling attacks on shipboard networked control systems*. 2015 Resilience Week (RWS), Philadelphia, PA, USA, 2015, pp. 1-6.

Erstad, E., Ostnes, R. and Lund, M.S. (2021). An operational approach to maritime cyber resilience. *TransNav*. 15(1): 27–34.

Fitton, M.O., Prince, D. and Lacy, M. (2015). *The Future of Maritime Cyber Security: Science and Technology.* Lancaster University.

Hareide, O.S., Jøsok, Ø., Lund, M. S. and Ostnes, R. (2018). Enhancing navigator competence by demonstrating maritime cyber security. *Journal of Navigation*. 71(5): 1025–1039.

Hatmi, A., Manteghi, M. and Khamseh, A. (2024). Identification of influencing factors on the informal advanced technology transfer using a qualitative approach in the industry LNG. Journal of Industrial and Systems Engineering, 16(3), 63-78.

Heering, D., Maennel, O. M. and Venables, A. N. (2021). Shortcomings in cybersecurity education for seafarers. developments in maritime technology and engineering. *Proceedings of the 5th International Conference on Maritime Technology and Engineering*. 1: 49–61. Düzenleyen: MARTECH 2020.

Hemminghaus, C., Bauer, J. and Padilla, E. (2021). Brat: A bridge attack tool for cyber security assessments of maritime systems. *TransNav.* 15(1): 35–44.

Herr, T. (2014). PrEP: A framework for malware and cyber weapons. *Journal of Information Warfare.*

Hopcraft, R., Harish, A. V., Tam, K. and Jones, K. (2023). Raising the standard of maritime voyage data recorder security. *Journal of Marine Science and Engineering*. 11(2).

Ibrahim, R.F., Abu Al-Haija, Q. and Ahmad, A. (2022). DDoS attack prevention for internet of thing devices using ethereum blockchain technology. *Sensors*. 22(18).

Kampourakis, V., Gkioulos, V. and Katsikas, S. (2023). A systematic literature review on wireless security testbeds in the cyber-physical realm. *Computers and Security.* Elsevier Ltd.

Kanwal, K., Shi, W., Kontovas, C., Yang, Z. and Chang, C. H. (2022). Maritime cybersecurity: are onboard systems ready? *Maritime Policy and Management.*

Kaur, R., Gabrijelčič, D. and Klobučar, T. (2023). Artificial intelligence for cybersecurity: literature review and future research directions. *Information Fusion.* 97.

Kolb, S.M. (2012). Grounded theory and the constant comparative method: valid research strategies for educators. *Journal of Emerging Trends in Educational Research and Policy Studies.*

Kushal, T.R.B., Lai, K. and Illindala, M.S. (2018). Risk-Based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system. *IEEE Transactions on Smart Grid.* 10(5): 4741–4750.

Kustanto, A. (2023). Recommended LNG Commercialization Strategy to Maintain Business Sustainability in the Global LNG Market. Unpublished Masters Thesis. Institut Teknologi Bandung.

Larsen, M.H. and Lund, M.S. (2021). Cyber risk perception in the maritime domain: a systematic literature review. *IEEE Access. Institute of Electrical and Electronics Engineers* Inc. ss. 144895–144905.

Larsen, M.H., Lund, M.S. and Bjørneseth, F.B. (2022). A model of factors influencing deck officers' cyber risk perception in offshore operations. *Maritime Transport Research*. 3.

Leong, P., Joseph, S.R.H. and Boulay, R. (2010). Applying constant comparative and discourse analyses to virtual worlds research. *Journal of Virtual Worlds Research*. 3(1).

Liu, Y., Ning, P. and Reiter, M.K. (2011). False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security.*

Longo, G., Orlich, A., Musante, S., Merlo, A. and Russo, E. (2023). MaCySTe: A virtual testbed for maritime cybersecurity. *SoftwareX*. 23.

Lutzhoft, M., Hynnekleiv, A., Earthy, J. V. and Petersen, E. S. (2019). Human-Centred maritime autonomy-an ethnography of the future. *Journal of Physics: Conference Series.* 1357(1).

Magsamen-Conrad K. and Dillon J. M. (2020). Mobile technology adoption across the lifespan: A mixed methods investigation to clarify adoption stages, and the influence of diffusion attributes, *Computers in Human Behavior,* Vol. 112, 106456, ISSN 0747-5632

Meland, P.H., Bernsmed, K., Wille, E., Rødseth, Ø. J. and Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents. *TransNav.* 15(3): 519 530.

Meng, Y., Khan, A., Bibi, S., Wu, H., Lee, Y. and Chen, W. (2021). The effects of COVID-19 risk perception on travel intention: evidence from chinese travelers. *Frontiers in Psychology.* 12.

Mittal, S. and Ilavarasan, P. V. (2019). Demographic factors in cyber security: an empirical study. Lecture Notes. *Computer Science*. 11701 LNCS, ss. 667–676.

Młody, M., Ratajczak-Mrozek, M. and Sajdak, M. (2023). Industry 4.0 technologies and managers' decision-making across value chain. evidence from the manufacturing industry. *Engineering Management in Production and Services.* 15(3): 69–83.

Mohan, V.S., Vinayakumar, R., Soman, K.P. and Poornachandran, P. (2018). S.P.O.O.F net: syntactic patterns for identification of ominous online factors. *Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops.* (ss. 258–263). Düzenleyen: SPW 2018. Institute of Electrical and Electronics Engineers Inc.

Mudra, G., Cui, H. and Johnstone, M.N. (2023). Survey: an overview of lightweight RFID authentication protocols suitable for the maritime internet of things. *Electronics* (Switzerland). 12(13).

Norton. (2018). What is a Trojan?. https://asia.norton.com/blog/malware/what is-a-trojan, Access Date: 22.10.2018.

Nurse, J. R. C., Creese, S. and De Roure, D. (2017). Trusting the internet of things security risk assessment in internet of things systems. *IEEE Computer Society.*

Odeh, A., Keshta, I. and Abdelfattah, E. (2020). Efficient detection of phishing websites using multilayer perception. *International Journal of Interactive Mobile Technologies.* 14(11): 22–31.

Onyeaka, H.K., Romero, P., Healy, B. C. and Celano, C. M. (2021). Age differences in the use of health information technology among adults in the united states: an analysis of the health information national trends survey. *Journal of Aging and Health*. 33(1–2): 147–154.

Oruc, A., Gkioulos, V. and Katsikas, S. (2022). Towards a cyber-physical range for the integrated navigation system (INS). *Journal of Marine Science and Engineering.* 10(1).

Paolucci, F., Civerchia, F., Sgambelluri, A., Giorgetti, A., Cugini, F. and Castoldi, P. (2019). P4 edge node enabling stateful traffic engineering and cyber security. *Journal of Optical Communications and Networking*. 11(1): 84-95.

Piccinelli, M. and Gubian, P. (2013). Modern ships voyage data recorders: a forensics perspective on the costa concordia shipwreck. *Proceedings of the Digital Forensic Research Conference*. (ss. 41–49). Düzenleyen: DFRWS 2013.

Progoulakis, I., Rohmeyer, P. and Nikitakos, N. (2021). Cyber physical systems security for maritime assets. *Journal of Marine Science and Engineering*. 9(12).

Sahay, R., Meng, W., Estay, D. A. S., Jensen, C. D. and Barfod, M. B. (2019). CyberShip-IoT: a dynamic and adaptive sdn-based security policy enforcement framework for ships. *Future Generation Computer Systems.* 100: 736–750.

Sarker, I.H. (2021). Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. *SN Computer Science*. 2(3).

Silverajan, B., Ocak, M. and Nagel, B. (2018). Cybersecurity attacks and defences for unmanned smart ships. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData).* (ss. 15–20). IEEE.

Skobelev, P., Skobelev, P.O. and Borovik, S.Y. (2017). On the way from industry 4.0 to industry 5.0: from digital manufacturing to digital society. *International Scientific Journal "Industry 4.0".* 307-311

Slovic, P. (2016). The perception of risk. scientists making a difference: one hundred eminent behavioral and brain scientists talk about their most important contributions. *Cambridge University Press.* ss. 179–182.

Smith, A., Papadaki, M. and Furnell, S.M. (2013). IFIP AICT 406 - improving awareness of social engineering attacks. *IFIP AICT.*

Tam, K., Jones, K.D. and Papadaki, M. (2012). Threats and impacts in maritime cyber security. *Engineering and Technology Reference*. 1(1).

Voinson, M., Billiard, S. and Alvergne, A. (2015). Beyond rational decision-making: modelling the influence of cognitive biases on the dynamics of vaccination coverage. *PLoS ONE.* 10(11).

Wang, C. N., Yang, F. C., Vo, N. T. M. and Nguyen, V. T. T. (2022). Wireless communications for data security: efficiency assessment of cybersecurity industry, a promising application for UAVs. *Drones.* 6(11)

Yeboah-Ofori, A. and Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. *Future Internet.* 11(3).

Yoo, J. and Jo, Y. (2023). Formulating cybersecurity requirements for autonomous ships using the square methodology. *Sensors.* 23(11).

Zagan, R., Raicu, G. and Sabau, A. (2022). Studies and research regarding vulnerabilities of marine autonomous surface systems (mass) and remotely operated vessels (rovs) from point of view of cybersecurity. *International Journal of Modern Manufacturing Technologies.* 14(3): 310–318.

Zeng, H., Zhao, Y., Wang, T. and Zhang, J. (2022). defense strategy against false data injection attacks in ship DC microgrids. *Journal of Marine Science and Engineering.* 10(12).

Zong, Y. and Zhao, X. (2018). Application discussion of source coding standard in voyage data recorder. *AIP Conference Proceedings*. (ss. 1955). AIP.