

A REVIEW OF CONTEMPORARY CYBER THREATS IN SHIP-TO-SHORE COMMUNICATIONS

LTJG Assist. Prof. Nadezhda Vladimirova¹⁾

¹⁾*Nikola Vaptsarov Naval Academy (Bulgaria)*

DOI : <https://doi.org/10.63662/c5eqpr67>

Abstract. This paper comprehensively reviews contemporary cyber threats focusing on critical ship-to-shore communications and advanced maritime surveillance systems. This study's purpose is to identify key vulnerabilities and propose effective mitigation strategies to enhance cyber resilience in the marine sector. The findings indicate a significant increase in cyber-attacks that compromise communication protocols and threaten data integrity. Practical implications include the necessity for continuous updates to cybersecurity protocols and the adoption of robust encryption methods. The originality of this work lies in its integration of empirical findings and expert perspectives from existing studies, informing a strong and adaptable security framework tailored to the unique challenges of the maritime industry. This paper deepens the understanding of maritime cyber threats and establishes a foundation for future research and policy development to fortify naval cybersecurity.

Keywords: maritime cyber threats; ship-to-shore communications; maritime surveillance systems; communication vulnerabilities; cyber resilience

1. Introduction

The maritime industry is a vital component of global trade, responsible for transporting over 80% of the world's goods by volume (Okumus et al., 2024). Its immense scale underscores its critical role in maintaining international trade and economic stability. However, as the sector embraces digital transformation, it faces growing cybersecurity challenges that threaten its operations. The integration of advanced technologies such as satellite communications (SATCOM), Very Small Aperture Terminals (VSAT), Automatic Identification Systems (AIS), and Global Navigation Satellite Systems (GNSS) enhances efficiency and safety but also introduces vulnerabilities that malicious actors can exploit (Akpan et al., 2022). The interconnected nature of maritime communication systems means that a cyber-attack on one component can cascade through the entire infrastructure, jeopardizing vessel safety, navigation, and cargo management. Disruptions to satellite communications, for instance, could lead to loss of navigational data and pose significant risks of accidents or environmental disasters. The global nature of the maritime industry amplifies the potential impact of cyber incidents, with vulnerabilities in one region affecting operations worldwide. The COVID-19 pandemic further highlighted these risks, as the maritime sector experienced a 400% increase in reported cyber incidents due to accelerated digitalization and increased reliance on remote operations (Lallie et al., 2021).

This paper explores the current landscape of cyber threats in maritime operations, focusing on the vulnerabilities within communication systems. By analyzing the nature and impact of these threats, the study aims to propose comprehensive mitigation strategies that enhance cyber

resilience. These strategies are essential not only for protecting individual vessels and ports but also for ensuring the stability and security of global trade networks.

2. Cyber Threats in Maritime Operations

The maritime industry, while being the backbone of global trade, faces significant cybersecurity challenges due to the digital transformation that has permeated every aspect of its operations. As vessels and shore facilities increasingly rely on interconnected digital systems for communication, navigation, and operations, they have become attractive targets for cybercriminals. This section delves into the various cyber threats that plague maritime operations, with a focus on the vulnerabilities in ship-to-shore communication systems and maritime surveillance technologies.

2.1 Overview of Maritime Communication Systems

Ship-to-shore communications enable real-time data exchange essential for maritime operations. However, vulnerabilities exist across core systems:

Table 1. Maritime Communication Systems (Source: developed by the author).

Systems	Functionality	Common Vulnerabilities
Satellite Communications (SATCOM)	Long-range communication for voice, data, and video transmission.	Signal interference, jamming
Very Small Apertures Terminals (VSAT)	Provides broadband internet, VoIP, and real-time data exchange.	Weak encryption, outdated software.
Automatic Identification Systems (AIS)	Tracks and identifies vessels for collision avoidance and traffic management.	Signal spoofing, false vessel identities
Global Navigation Satellite Systems (GNSS)	Provides accurate positioning and timing for navigation.	Spoofing and jamming

- **Satellite Communications (SATCOM):** SATCOM systems are essential for maintaining long-range communication between ships and shore-based operations. These systems facilitate the transmission of voice, data, and video, supporting everything from navigation to crew welfare. However, their reliance on satellite links makes them susceptible to targeted attacks, such as signal interference or jamming, which can disrupt the flow of information and potentially lead to dangerous situations at sea.

- **Very Small Aperture Terminals (VSAT):** VSAT networks are widely used in the maritime industry to provide broadband connectivity for vessels. These systems support a range of applications, including internet access, VoIP, and real-time data exchange. Due to their use of small, dish-like antennas to communicate with satellites, VSAT systems are vulnerable to cyber-attacks that exploit weak encryption or outdated software, potentially leading to unauthorized access or data breaches (*NSA Issues Recommendations to Protect VSAT Communications* > *National Security Agency/Central Security Service* > *Article* [no date])

- **Automatic Identification Systems (AIS):** AIS is a crucial safety tool used to track and identify vessels in real time. It transmits information such as the ship's name, position, course, and speed, which is essential for collision avoidance and traffic management. However, AIS is

not immune to cyber threats. Attackers can spoof AIS signals, creating false vessel identities or positions, which can result in collisions or other maritime incidents

- **Global Navigation Satellite Systems (GNSS):** GNSS, including the widely used GPS, provides accurate positioning and timing information for vessels. This system is fundamental to modern navigation. However, GNSS signals are vulnerable to spoofing and jamming attacks, which can mislead a vessel's navigation system, causing it to veer off course or misinterpret its location (*GNSS* [no date]).

These communication systems, while advanced, are interconnected in ways that create multiple entry points for cyber-attacks. The interdependence of these technologies means that an attack on one component can have cascading effects on the entire maritime operation, leading to significant disruptions.

Despite their advantages, these systems' interdependence creates multiple entry points for cyber-attacks. For instance, a disruption in SATCOM could lead to the loss of critical navigational data, endangering vessel safety.

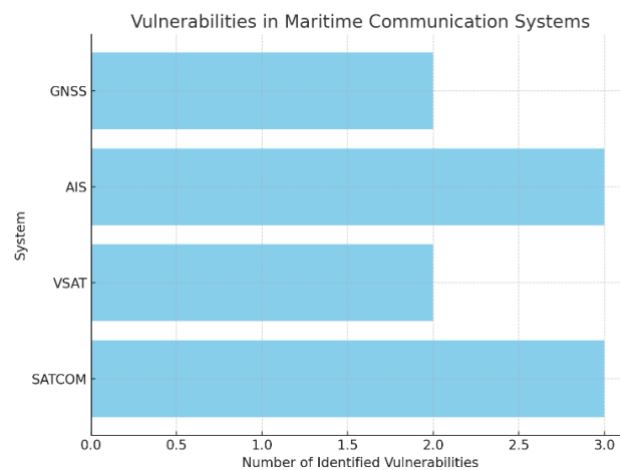


Figure 1. Vulnerabilities in Maritime Communication Systems

Proposed Solutions:

1. **Advanced Encryption:** Use Quantum Key Distribution (QKD) or AES-256 encryption for secure transmissions.
2. **Anti-Jamming Technologies:** Deploy technologies to detect and mitigate signal interference in SATCOM and GNSS systems.
3. **Redundancy Plans:** Integrate backup systems like LORAN-C for continues operation during GNSS outages.
4. **Authentication Protocols:** Employ real-time AIS signal validation to prevent spoofing attacks.

2.2 Key Cyber Threats and Incident Data

The maritime sector is increasingly under siege from a range of sophisticated cyber threats. These threats target not only communication systems but also the broader operational technologies that support maritime activities. This section highlights the most pressing cyber threats that maritime operators must contend with, supported by practical examples.

2.2.1 Phishing and Social Engineering

Phishing and social engineering attacks are among the most widespread threats in the maritime industry. These tactics often involve cybercriminals manipulating individuals into revealing sensitive information or unknowingly installing harmful software on crucial systems.

A recent case highlighted a phishing campaign that targeted the email accounts of crew members aboard a large cargo vessel. The attackers, masquerading as port authorities, sent emails containing malicious links disguised as official documents required for port entry. Once the links were clicked, malware was deployed onto the vessel's network, granting unauthorized access to its navigation and communication systems. This breach not only undermined the ship's operational security but also endangered the safety of the crew and cargo. (*Phishing Emails Impersonate Maritime Industry in Likely BEC Campaign* [no date]).

Such incidents underscore the importance of cybersecurity awareness and training among maritime personnel. Implementing rigorous email filtering systems and educating crew members on the dangers of phishing can mitigate the risks posed by these types of attacks. Phishing attacks often exploit human error. A case involving crew members targeted by fraudulent emails led to malware installation and unauthorized access to navigation systems.

Table 2. Phishing attacks

Year	Incident	Impact
2020	Phishing campaign on a cargo vessel	Malware breached navigation systems
2021	Social engineering attack on port staff	Unauthorized access to operational networks

2.2.2 Malware and Ransomware

Malware and ransomware attacks have become increasingly common in the maritime industry, with attackers often seeking to disrupt operations or extort money from companies. These types of attacks can have devastating consequences, particularly when they target critical communication and navigation systems.

A prominent example is the 2017 NotPetya ransomware attack on Maersk, one of the most well-known cyber-attacks in the maritime sector. The attack crippled Maersk's IT infrastructure, forcing the company to reinstall thousands of servers and workstations across its global network. The disruption caused Maersk to halt operations at several ports, resulting in an estimated \$300 million in losses (Maersk CISO Says NotPeyta Devastated Several Unnamed US Firms [no date];).

The attack highlighted the vulnerability of even the largest and most technologically advanced shipping companies to cyber threats.

To prevent such incidents, maritime organizations must adopt robust cybersecurity measures, including regular system updates, the use of advanced threat detection software, and comprehensive backup strategies to ensure that data can be recovered quickly in the event of an attack.

Table 3. Significant cyber incidents in the maritime industry.

Year	Type of attack	Impact	Affected Organization
2017	Ransomware (NotPetya)	\$ 300M loss, global operation halt	Maersk
2021	Malware	Operational delays, data breaches	Multiple shipping firms

2.2.3 DDOS Attacks

DDoS attacks occur when attackers flood networks with excessive traffic, rendering systems inoperable. In the maritime context, such attacks often target:

- **Port Authorities:** Cybercriminals overwhelm port IT infrastructures, delaying cargo handling and disrupting logistical chains.
- **Maritime Traffic Management Systems:** These systems become unresponsive, leading to navigational risks as vessels cannot receive crucial routing updates.
- **Ship IT Networks:** Onboard systems relying on internet connectivity, such as satellite links, can be overwhelmed, causing disruptions to communications and navigation.

Real-Life Example: In 2020, a port in Europe experienced a significant DDoS attack during peak operations, delaying vessel departures and causing economic losses. This attack highlighted the vulnerabilities of port infrastructures that depend on digital systems for scheduling and management. (Clavijo Mesa et al. 2024)

Mitigation Measures:

- Deploy DDoS protection tools that identify and filter malicious traffic.
- Establish redundant communication channels, including manual operations, to minimize disruptions during an attack.
- Regularly test network capacity and implement load-balancing systems.

2.2.4 DNS Spoofing

DNS spoofing (or DNS cache poisoning) manipulates the Domain Name System (DNS) to redirect traffic intended for legitimate servers to malicious ones. In maritime applications, attackers can:

- **Intercept Communications:** Redirect ship-to-shore communications, exposing sensitive navigation and cargo data.
- **Fake Port Authority Systems:** Present fraudulent interfaces for customs declarations, leading to unauthorized access or financial theft.
- **Disrupt E-Navigation Systems:** Redirect data from AIS or ECDIS systems, potentially causing collisions or vessel misrouting.

Real-Life Example: In 2021, DNS spoofing was used to impersonate a port authority's customs declaration system. Ship operators unknowingly provided sensitive shipping manifests, which were subsequently used for illegal activities. (DNS Poisoning (DNS Spoofing): Definition, Technique & Defense | Okta [no date])

Mitigation Measures:

- Implement DNS Security Extensions (DNSSEC) to authenticate DNS responses.
- Use encrypted connections like HTTPS and VPNs for critical maritime communications.
- Monitor DNS traffic for anomalies and maintain regular DNS cache clearing.

2.2.5 Software Supply chain attacks

Supply chain attacks exploit vulnerabilities in third-party software used by maritime organizations. Attackers can:

- **Embed Malware:** Introduce malicious code during software updates or installations for navigation systems, AIS, or crew welfare software.
- **Compromise Operational Technology (OT):** Exploit vulnerabilities in ship systems like propulsion or cargo handling software.
- **Create Backdoors:** Enable unauthorized remote access to ship IT systems via compromised software.

Real-Life Example: In 2021, a shipping firm's navigation software was unknowingly infected during a routine update. The malware disrupted vessel tracking and communication systems, resulting in operational delays. (Sobb et al. 2020)

Mitigation Measures:

- Verify the authenticity and integrity of all software updates using cryptographic signatures.
- Conduct regular vulnerability assessments on third-party software.
- Implement application whitelisting to block unauthorized software execution.
- Require suppliers to follow strict cybersecurity standards, such as ISO/IEC 27001.

2.2.6 GPS Spoofing and Jamming

GPS spoofing and jamming are particularly concerning in the maritime context because of their potential to cause navigational errors that can lead to serious accidents. These attacks involve either the transmission of false GPS signals to mislead navigation systems or the jamming of legitimate signals, rendering them unusable. For example, in 2017, a commercial vessel in the Black Sea reported a GPS spoofing incident where the ship's navigation system indicated that it was located miles inland, rather than at sea. This discrepancy confused the crew and could have led to a collision if not quickly identified and corrected. Such incidents are becoming more frequent, particularly in geopolitically sensitive regions where state-sponsored actors may use GPS spoofing as a means of disrupting maritime traffic (Grison 2023).

Mitigating these risks requires the development and deployment of anti-jamming and anti-spoofing technologies, as well as the implementation of alternative navigation systems that can serve as backups in the event of a GPS failure.

2.2.6 Man-in-the-Middle (MitM) Attacks

Man-in-the-middle (MitM) attacks are sophisticated cyber-attacks where the attacker intercepts and potentially alters communications between two parties without their knowledge. In the maritime industry, such attacks can compromise the integrity of communication between a vessel and shore-based operations. For example, a notable MitM attack occurred when cybercriminals intercepted communication between a container ship and its management office. By inserting themselves into the communication channel, the attackers manipulated cargo manifests, resulting in the misplacement of valuable cargo and significant financial losses for the shipping company. This breach also exposed sensitive information about the ship's itinerary and cargo, which could have been used for further criminal activities (DNV 2023).

To defend against MitM attacks, maritime operators should implement strong encryption protocols for all communications and regularly update security certificates to prevent unauthorized access.

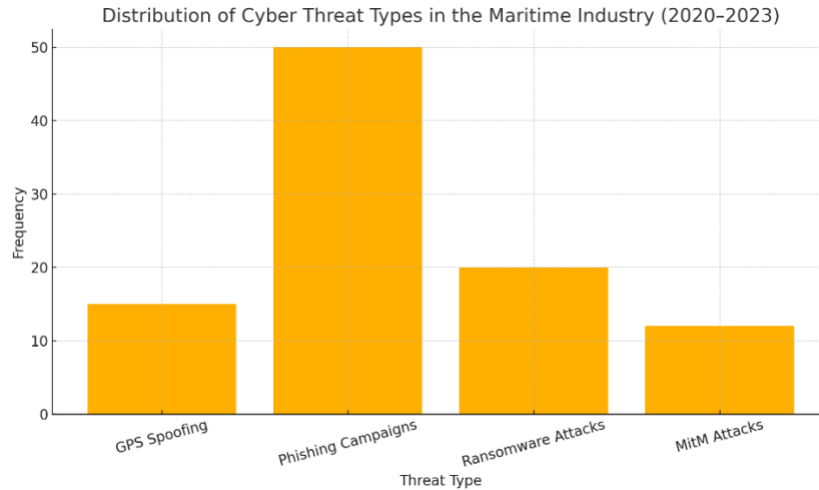


Figure 2. Distribution of cyber threat types in the Maritime industry (2020-2023).

2.3 Vulnerabilities in Maritime Surveillance Systems

Maritime surveillance systems, including radar, AIS, and Electronic Chart Display and Information Systems (ECDIS), face unique challenges. For example, a 2021 AIS spoofing attack created “ghost ships” on radar screens, confusing nearby crews and escalating collision risks (Androjna et al. 2021).

Table 4. Vulnerabilities in Maritime Surveillance Systems.

System	Vulnerability	Impact
AIS	Signal manipulation	Phantom vessels causing confusion
Radar	Signal jamming	Loss of situational awareness
ECDIS	Malware infection	Inaccurate navigational data

To protect maritime surveillance systems from cyber threats, it is essential to implement layered security measures, including network segmentation, intrusion detection systems, and regular security audits. Additionally, investing in training for crew members on how to recognize and respond to potential cyber threats can further enhance the security of these critical systems.

3. Mitigation Strategies for Enhancing Cyber Resilience

The maritime industry faces an increasingly complex cybersecurity landscape, requiring a multi-faceted approach to mitigate the wide array of threats effectively. This section outlines the key strategies for strengthening the industry's cybersecurity defenses, emphasizing the importance of regulatory frameworks, skill development, and technological advancements. Each strategy is discussed with practical examples and real-world applications to provide a comprehensive understanding of their significance.

3.1 Strengthening Regulatory Frameworks

The regulatory landscape for maritime cybersecurity is currently fragmented, with varying standards and practices across different regions and authorities. This lack of uniformity creates vulnerabilities as inconsistent practices can lead to gaps in security that cybercriminals may exploit. A harmonized approach to cybersecurity regulations is essential for ensuring all stakeholders adhere to consistent standards, enhancing the maritime industry's overall resilience.

For instance, the International Association of Classification Societies (IACS) has recognized the need for standardized cybersecurity practices and has introduced the Unified Requirements (UR) E26 and E27, which focus on the cyber resilience of ships and systems. UR E26 addresses the cyber resilience of ships, covering aspects such as network segmentation, access control, and incident response planning. UR E27, on the other hand, focuses on the cybersecurity of maritime systems and equipment, ensuring that they meet specific security requirements before being installed on ships (*Addressing cyber resilience of ships - Press - IACS* [no date]).

The implementation of these requirements is mandatory for all IACS members, who represent over 90% of the world's commercial fleet. By adopting these standards, the industry can ensure a consistent level of cybersecurity across the global maritime sector, reducing the likelihood of vulnerabilities due to disparate regulatory practices.

In response to the introduction of UR E26 and E27, several shipbuilding companies have begun to incorporate these cybersecurity requirements into their design and construction processes. For example, a major shipyard in South Korea has developed a comprehensive cybersecurity framework based on IACS guidelines, ensuring that all new vessels are built with robust cybersecurity measures from the outset. This proactive approach enhances the ship's security and sets a new industry standard (*Maritime cyber security: Mandatory IACS Unified Requirements for shipyards and suppliers from July 2024* [no date]).

Furthermore, the European Union's Network and Information Systems Directive (NIS2) has extended its scope to include maritime transport, requiring member states to implement cybersecurity measures for operators of essential services, including ports and shipping companies (*Cybersecurity of network and information systems (2022)* [no date]). This directive aligns with international standards and encourages cooperation among EU countries to address cybersecurity threats more effectively.

3.2 Skill Development

One of the most significant challenges facing the maritime industry is the critical shortage of cybersecurity professionals with the necessary skills to protect against sophisticated cyber threats. The maritime sector has traditionally focused on physical security, and the shift towards digitalization has outpaced the development of corresponding cybersecurity expertise. Addressing this skills gap is crucial for building a resilient cybersecurity workforce capable of defending maritime operations.

To address this issue, the European Maritime Safety Agency (EMSA) has recognized this challenge and has taken steps to address the cybersecurity skills gap within the industry. EMSA has developed a specialized training program for maritime inspectors and other relevant stakeholders, focusing on cybersecurity risk management, incident response, and best practices for maritime cybersecurity. The program includes both online and in-person components, ensuring that participants gain practical experience in addition to theoretical knowledge (*Cybersecurity in the Maritime Sector: ENISA Releases New Guidelines for Navigating Cyber Risk — ENISA* [no date]).

EMSA has also collaborated with several maritime academies across Europe to integrate cybersecurity modules into their curricula. This initiative aims to equip the next generation of maritime professionals with the skills needed to address cybersecurity challenges from the start of their careers. Additionally, EMSA has partnered with industry leaders to offer internships and hands-on training opportunities, providing students with real-world experience in maritime cybersecurity (*Latest News - EMSA holds 2023 Maritime Cybersecurity Conference - EMSA - European Maritime Safety Agency* [no date]).

Furthermore, the concept of continuous professional development (CPD) is being promoted within the industry. Maritime organizations are encouraged to invest in ongoing training for their existing workforce, ensuring that employees remain up to date with the latest cybersecurity threats and defenses. For example, a leading shipping company has implemented a CPD program that includes regular cybersecurity workshops, certifications, and simulated cyber-attack drills to keep their crew and shore-based staff prepared for potential incidents (*Latest News - EMSA holds 2023 Maritime Cybersecurity Conference - EMSA - European Maritime Safety Agency* [no date]).

3.3 Technological Advancements

Enhancing cybersecurity in maritime operations requires adopting advanced technologies and best practices to address evolving threats. Key measures include implementing encryption techniques, network segmentation, real-time monitoring, and incident response planning.

Encryption such as Quantum Key Distribution (QKD) ensures secure ship-to-shore communications, making data interception nearly impossible (Akpan et al., 2022). Network segmentation divides ship networks into isolated segments (e.g., navigation, communication, operational technology), limiting attackers' lateral movement. A global shipping company successfully adopted this strategy, coupled with AI-powered real-time monitoring to detect and respond to threats swiftly.

Incident response planning is critical. For example, a Northern European port conducts quarterly drills simulating cyber-attacks like ransomware and GPS spoofing, ensuring readiness across teams (CRIMSON III). Additionally, cybersecurity hygiene practices—such as regular software updates, multi-factor authentication (MFA), and strict access control—significantly reduce vulnerabilities. (*Service for Foreign Policy Instruments Critical Maritime Routes Programme Monitoring, Support and Evaluation Mechanism (CRIMSON III) Cybersecurity in Maritime Critical Infrastructure Reflection on African Ports* [no date]) .

These measures collectively enhance maritime cybersecurity, ensuring resilient operations in the face of rising cyber threats.

3. Conclusion

This study highlights significant vulnerabilities in ship-to-shore communications and maritime surveillance systems. Key threats, including phishing, ransomware, GPS spoofing, DDoS, DNS spoofing, MitM attacks, and software supply chain attacks, underscore the need for robust defenses. While current mitigation strategies align with regulatory standards, the integration of advanced technologies like AI monitoring and QKD encryption can further bolster resilience.

Future research should focus on testing the resilience of maritime communication signals and exploring innovative cybersecurity frameworks tailored to the sector's unique challenges. Addressing these gaps will ensure the continued security and stability of global maritime operations.

REFERENCES

AKPAN, F. et al., 2022. Cybersecurity Challenges in the Maritime Sector. *Network*, vol. 2, no. 1, pp. 123–138. ISSN 2673-8732. Available from: <https://doi.org/10.3390/NETWORK2010009>. [viewed 2024-08-15].

AKPAN, F. et al., 2022. Cybersecurity Challenges in the Maritime Sector. *Network*, vol. 2, no. 1, pp. 123–138. ISSN 2673-8732. Available from: <https://doi.org/10.3390/NETWORK2010009>. [viewed 2024-08-16].

ANDROJNA, A. et al., 2021. AIS Data Vulnerability Indicated by a Spoofing Case-Study. *Applied Sciences*, vol. 11, no. 11, pp. 5015. ISSN 2076-3417. Available from: <https://doi.org/10.3390/APP11115015>. [viewed 2024-08-17].

CLAVIJO MESA, M. V. et al., 2024. Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains. *Information*, vol. 15, no. 11, pp. 710. ISSN 2078-2489. Available from: <https://doi.org/10.3390/INFO15110710>. [viewed 2024-08-12].

Cyber Threats and Choke Points: How Adversaries are Leveraging Maritime Cyber Vulnerabilities for Advantage in Irregular Warfare - Modern War Institute, [no date]. Web Site. Available from: <https://mwi.westpoint.edu/cyber-threats-and-choke-points-how-adversaries-are-leveraging-maritime-cyber-vulnerabilities-for-advantage-in-irregular-warfare/>. [viewed 2024-08-15].

Cybersecurity in the Maritime Sector: ENISA Releases New Guidelines for Navigating Cyber Risk — ENISA, [no date]. Web Site. Available from: <https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-maritime-sector-enisa-releases-new-guidelines-for-navigating-cyber-risk>. [viewed 2024-08-17].

Cybersecurity of network and information systems (2022), [no date]. Web Site. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4637829>. [viewed 2024-08-19].

DNS Poisoning (DNS Spoofing): Definition, Technique & Defense | Okta, [no date]. Web Site. Available from: <https://www.okta.com/identity-101/dns-poisoning/>. [viewed 2024-08-12].

DNV, 2023. MARITIME CYBER PRIORITY 2023.

GNSS, [no date]. Web Site. Available from: <https://www.unoosa.org/oosa/en/ourwork/psa/gnss/gnss.html>. [viewed 2024-08-10].

LALLIE, H. S. et al., 2021. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers and Security*, vol. 105. ISSN 0167-4048. Available from: <https://doi.org/10.1016/J.COSE.2021.102248>.

Latest News - EMSA holds 2023 Maritime Cybersecurity Conference - EMSA - European Maritime Safety Agency, [no date]. Web Site. Available from: <https://www.emsa.europa.eu/we-do/safety/maritime-security/item/5053-emsa-holds-2023-maritime-cybersecurity-conference.html>. [viewed 2024-08-12].

Maersk CISO Says NotPetya Devastated Several Unnamed US firms, [no date]. Web Site. Available from: <https://www.darkreading.com/cyber-risk/maersk-ciso-says-notpetya-devastated-several-unnamed-us-firms>. [viewed 2024-08-06].

Maritime cyber security: Mandatory IACS Unified Requirements for shipyards and suppliers from July 2024, [no date]. Web Site. Available from: <https://www.dnv.com/maritime/webinars-and-videos/on-demand-webinars/access/maritime-cyber-security-mandatory-iacs-ur-for-newbuilds-from-july2024-30may/>. [viewed 2024-08-12].

NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs | ZDNET, [no date]. Web Site. Available from: <https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/>. [viewed 2024-08-06].

NSA Issues Recommendations to Protect VSAT Communications > National Security Agency/Central Security Service > Article, [no date]. Web Site. Available from: <https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2910409/nsa-issues-recommendations-to-protect-vsats-communications/>. [viewed 2024-08-09].

OKUMUS, D. et al., 2024. An Approach to Advance Circular Practices in the Maritime Industry through a Database as a Bridging Solution. *Sustainability*, vol. 16, no. 1, pp. 453. ISSN 2071-1050. Available from: <https://doi.org/10.3390/SU16010453>. [viewed 2024-08-15].

Phishing Emails Impersonate Maritime Industry in Likely BEC Campaign, [no date]. Web Site. Available from: <https://blog.electiciq.com/phishing-emails-impersonate-maritime-industry-in-likely-bec-campaign>. [viewed 2024-08-05].

Service for Foreign Policy Instruments Critical Maritime Routes Programme Monitoring, Support and Evaluation Mechanism (CRIMSON III) Cybersecurity in Maritime Critical Infrastructure Reflection on African Ports, [no date].

SOBB, T. et al., 2020. Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. *Electronics*, vol. 9, no. 11, pp. 1864. ISSN 2079-9292. Available from: <https://doi.org/10.3390/ELECTRONICS9111864>. [viewed 2024-08-12].

LTJG Assist. Prof. Nadezhda Vladimirova

ORCID iD: 0000-0001-7831-2395

Nikola Vaptsarov Naval Academy

Varna, Bulgaria

E-mail: n.vladimirova@nvna.eu

