Cyber Incident Scenarios in the Maritime Industry: Risk Assessment and Mitigation Strategies

Mohamed Ben Farah, M. Omar Al-Kadri, Yussuf Ahmed, Raouf Abouzariba, *Dpt. of Networks and Cybersecurity*
Birmingham City University, Birmingham, B4 7XG, UK.
{Mohamed.Benfarah, Omar.Alkadri, Yussuf.Ahmed, Raouf.Abozariba}@bcu.ac.uk
Xavier Bellekens, *Lupovis Limited*
Glasgow, UK
xavier@lupovis.io

2023 IEEE International Conference on Cyber Security and Resilience (CSR) | 979-8-3503-1170-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/CSR57506.2023.10224972

***Abstract*—The maritime industry is facing an escalating concern of cybersecurity threats, which can be attributed to the rapid growth of digital technologies and the recent adoption of autonomous and semi-autonomous shipping. To address this issue, various published papers have proposed cyberattack scenarios aiming to increase cybersecurity awareness and enhance the security of maritime systems. This research aims to assess the cybersecurity threats in the maritime sector by presenting three practical cyberattack scenarios and their corresponding risks and mitigation strategies. The first scenario involves the risks associated with utilizing the systems of a tug-boat as part of an attack vector, the second scenario examines the systems involved in vessel harbour manoeuvres using a laser docking system or Radar, and the third scenario examines an insider attack through malicious or unauthorized access to the Berthing Aid System (BAS).**

I. Introduction

The reliability and sustainability of the maritime industry play a vital role in the economic success of nations worldwide. Vessels serve as critical transportation systems, used for importing and exporting goods across the globe. Ensuring safety and security within the maritime industry heavily relies on the implementation of robust cybersecurity measures and solutions to protect against cyberattacks. Additionally, in markets where there is a high demand for sustainable development, low-cost operations, and efficiency, the maritime industry carries out 90% of the transportation of all goods [1], [2]. Recent research shows that information system solutions such as IoT, big data and machine learning are significantly applied to the maritime sector, opening new horizons for the maritime infrastructure's digital transformation [3], [4]. Furthermore, the connectivity to smart devices, using satellite and GPS, attracts cyber-criminals to attempt cyberattacks such as social engineering and man-in-the-middle.

To minimize the risk of cyberattacks and safeguard maritime companies' data and networks from malicious cyberthreats, increasing maritime cybersecurity awareness is crucial. As such, there has been a rise in published research papers proposing new cyberattack scenarios to improve cybersecurity awareness [5], [6]. Recent research has also highlighted the clear link between cybersecurity and autonomous vessels [7]–[10].

The maritime industry witnessed an increased use of navigation systems such as Automatic Identification Systems (AIS), Global Navigation Satellite Systems (GNSS), and Radio Detection and Ranging (RADAR). The use of such systems negatively impacts the security of maritime infrastructures. Furthermore, recent research has indicated that maritime companies are vulnerable to highly complex new types of cyberattacks that target both their information systems and vessels [11], [12].

Detecting potential cybersecurity threats in the maritime industry is an important step towards developing effective safety measures. In addition to identifying potential threats, maritime enterprises must also develop mitigation strategies to protect against cybersecurity hazards. While some scholarly articles such as [13], [14] have focused on classifying threats and conducting risk analysis in the maritime industry, they only cover certain aspects of the holistic scenario, with a focus on risk assessment which can be further improved with mitigation strategies. The contribution of this paper can be summarized as follows:

1) We present three realistic cyberattack scenarios covering various aspects involved in vessel operation. For each scenario, the paper provides a comprehensive risk assessment, highlighting the potential impact on vessel operations, cargo, and personnel.
2) We develop practical mitigation strategies, including network segmentation, system hardening, and authentication and encryption protocols for docking systems. We also propose access control and monitoring mechanisms to mitigate the risks associated with insider attacks.

The remainder of the paper is organized as follows; Section II details the presented cyberattack scenarios within the maritime industry. Section III presents each scenario's risk assessment and mitigation strategy. The radar data tampering simulation is presented in Section IV. Finally, conclusions are drawn in Section V.

II. Scenarios description

A. Tug boat cyberattack

Tug boats assist vessels in port manoeuvring and towing. However, with the increasing adoption of digital technologies and the Internet of Things (IoT), tug boats are becoming increasingly vulnerable to cyberattacks. In this scenario, we

TABLE I
DOCKING SYSTEM TYPES

Docking system	Components	Type
Shore based	– Laser sensors/ Ultrasounds/ Radar – Microwave transponders – Monitoring unit (Control room ashore) – Pilot's devices (Laptop/tablet/phone) – Wireless transmitter/receiver	Active
Shore based	– AIS – DGPS (2-3 m) accuracy – Gyro compass – Satellite receiver	Passive
Vessel-based	– PPU (Portable pilot's devices) – Laptop/Tablet (Docking Software) – ECDIS – AIS – DGPS – GPS compass	Active

consider the potential risks associated with an attacker compromising the systems of a tug boat and using them to launch a cyberattack. Such an attack could cause damage to the vessel, loss of cargo, and risks to personnel. Section III provides an insight of the systems involved in a tug-boat along with their associated risks. In response to these identified risks, practical mitigation strategies are proposed to help the maritime industry defend against such attacks.

B. Harbour manoeuvres incidents

Docking and maneuvering systems are a critical component of vessel operations, enabling safe and efficient harbor manoeuvres. In this scenario, we consider the potential risks associated with an attacker compromising the systems involved in a vessel's harbor manoeuvres and using them as attack vectors. There are two types of docking systems, shore-based systems, and vessel-based systems, and both present unique risks and vulnerabilities. The potential impact of a successful attack on these systems could cause damage to the vessel or associated system, loss of asset, and potential risks to personnel. Table I lists the components involved in the docking system, and Section III provides further details on the active and passive shore and vessel-based docking systems along with their associated risks, followed by potential risk mitigation strategies to strengthen the security of these components.

C. The employee accesses the Berthing Aid System (BAS)

Berthing involves demanding manoeuvres that can present a risk to the vessel and surrounding vessels. It is inherent for logistic companies to invest a considerable amount of money in preventing damages to the vessel due to direct impact against the dock. These accidents can cause loss of lives and damage to property. BASs reduces operational costs and damages to the dock by providing guided assistance to the pilots. These measures contribute to the vessel's safety through safe navigation and efficient security. The real-time data contains critical information that can become a target for attackers. In this scenario, the hackers can gain unauthorised access to the communication and controls systems which can negate the safety and security of the vessel through BAS. The attackers can also perform unauthorised modifications to the data, affecting the integrity of the information being relayed to the pilots. Such attacks can result in the loss of lives and substantial damage to the infrastructure.

III. Risk Assessment and Mitigation Methods

Maritime researchers have long recognized the critical importance of safety and security issues within the maritime sector, including those related to seafarer safety, transportation, and cargo security. However, as the nature of navigational safety and maritime security evolves, it is becoming increasingly evident that fostering a robust cybersecurity culture must be a top priority. This includes a focus on further developing and integrating cyber and information security measures into existing safety and security frameworks.

The International Maritime Organization (IMO) serves as the primary agency of the United Nations (UN) responsible for formulating policies and procedures aimed at ensuring safety and security within the maritime industry. These policies address various risks, including those posed by the maritime sector and environmental hazards. To protect vessels from potential cyberattacks, the IMO has established protocols and procedures that outline both preventative and corrective measures, incorporating key components of cyber risk management [15]. This section aims to provide a risk assessment associated with scenarios discussed in Section II. It also aims to define mitigation strategies, following findings from recent research works and the security standards such as IMO framework, which consists of five key elements: identification, protection, detection, response, and recovery.

A. Tug boat cyberattacks

The risks associated with tug boats can be categorized into the following areas:

1) Communication Systems: The communication systems used on tug boats to communicate with other vessels or shore-based facilities can be subject to cyberattacks, leading to a loss of communication or even a takeover of the systems. Cyberattacks on communication systems can take many forms, including jamming, spoofing, or interception of communication signals. Jamming can cause interference with the communication signals, making it difficult for the tug boat to communicate with other vessels or shore-based facilities. Spoofing can involve the use of false signals to trick the tug boat's communication systems into accepting unauthorized instructions, leading to incorrect actions or compromised safety. Interception can result in sensitive or confidential information being exposed to unauthorized third parties. To mitigate the risk of cyberattacks on communication systems, the following measures can be taken:
   - Deploy secure communication protocols, such as encryption and authentication, to protect against interception and spoofing, such as Secure Sockets Layer/Transport Layer Security (SSL/TLS), Message Digest 5 (MD5) and Secure Hash Algorithm (SHA), and Advanced Encryption Standard (AES).

- Install intrusion detection system (IDS) and/or intrusion prevention systems (IPS) to detect and block unauthorized access to communication systems.
- Conduct regular cybersecurity training for personnel to raise awareness of the risks associated with communication systems.

2) Navigation Systems: Tug boats rely on navigation systems to navigate safely and avoid collisions. These systems can be subject to cyberattacks that can interfere with the accuracy of the navigation systems, causing navigation errors and potentially endangering the safety of the vessel and crew. Navigation systems can be interfered with or overridden, causing navigation errors or collisions with other vessels. This can lead to significant damage, injury or loss of life. To mitigate the risk of cyberattacks on navigation systems, the following measures can be taken:
   - Implement secure navigation protocols that can resist interference or spoofing attacks. examples of such protocols include Global Positioning System (GPS) signal authentication which is used to verify the authenticity of the GPS signal by useing digital signatures. Differential GPS (DGPS), which is a technique that improves the accuracy of GPS by using a network of ground-based reference stations to broadcast correction signals to GPS receivers. This technique can help to mitigate the effects of interference or spoofing attacks by providing more accurate positioning information. eLoran, which is a radio navigation system that provides accurate timing and positioning information. It is designed to be resilient to interference and spoofing attacks by using multiple transmitters and signal diversity. And Inertial Navigation Systems (INS), which uses accelerometers and gyroscopes to measure the movement of the vessel.
   - Install backup navigation systems to reduce the impact of a cyberattack on the primary system such as INS.
   - Conduct regular assessments of the vessel's navigation systems to identify vulnerabilities and implement appropriate countermeasures.
   - Train personnel on how to identify and respond to navigation system cybersecurity incidents.

3) Operational Technology (OT) Systems: Tug boats are equipped with a variety of OT systems, such as engine control systems and propulsion systems. Cyberattacks on these systems can cause damage to the engines and propulsion systems or even complete loss of control of the tug boat. Cyberattacks on OT systems can have severe consequences for the tug boat's operations too. For example, if the engine control system is compromised, the tug boat may experience engine failures or erratic behaviour, leading to a loss of control of the vessel. Similarly, if the propulsion system is attacked, the tug boat may experience a loss of power or reduced manoeuvrability, which can compromise the safety of the vessel and crew. To mitigate the risk of cyberattacks on OT systems, the following measures can be taken:
   - Implement secure OT protocols that can resist unauthorized access or tampering.
   - Conduct regular assessments of the tug boat's OT systems to identify vulnerabilities and implement appropriate countermeasures.
   - Install intrusion detection and prevention systems to detect and block unauthorized access to OT systems.
   - Train personnel on how to identify and respond to OT system cybersecurity incidents.

4) Human factors: Cybersecurity incidents can also arise from human error or insider threats, where personnel may unwittingly or intentionally compromise the security of the tug boat systems. Human factors, including insider threats or human error, can also pose significant cybersecurity risks for tug boats. An insider threat can involve an employee or contractor with authorized access to the tug boat's systems who intentionally or unintentionally compromises the system's security. For example, an employee may introduce malware into the system, leading to a data breach or system failure. Human error can also lead to security breaches, such as the accidental release of sensitive information or the failure to follow proper cybersecurity procedures. To mitigate the risk of cybersecurity incidents resulting from human factors, the following measures can be taken:
   - Implement access controls to limit personnel access to systems and data.
   - Conduct regular background checks on personnel to identify potential insider threats.
   - Implement a security incident response plan that includes procedures for responding to cybersecurity incidents caused by human factors.
   - Conduct regular cybersecurity training to raise awareness of the risks associated with human factors.

B. Harbour manoeuvres incidents

In addition to the risks that are common to the tug scenario, there are risks that are specific to the vessel, particularly concerning its communication and manoeuvring capabilities within the harbour. The risk assessment and mitigation recommendations of the shore and vessel-based components are presented as follows:

Laser Sensors: Laser sensors use laser beams to detect the distance and position of objects. The cybersecurity risks associated with laser sensors are relatively low, as they are standalone devices that are not connected to any network or system. However, there is a risk of data interception or tampering during transmission, especially if the data is transmitted wirelessly. Therefore, proper encryption and secure transmission protocols should be used to prevent unauthorized access or data tampering.

Ultrasound: Ultrasound uses high-frequency sound waves to detect the position of objects. Like laser sensors, the cybersecurity risks associated with ultrasound are relatively low, as they are standalone devices. However, there is a risk of data interception or tampering during transmission.

Radar: Radar uses radio waves to detect the position and movement of objects. The cybersecurity risks associated with radar are also relatively low, as they are standalone devices that are not connected to any network or system. However, there is a risk of data interception or tampering during transmission, especially if the data is transmitted wirelessly. Therefore, proper encryption and secure transmission protocols should be used to prevent unauthorized access or data tampering. Additionally, radar can be subject to physical tampering or interference, such as jamming, which can disrupt the system's operation. Proper physical security measures should be implemented to prevent unauthorized access to the radar system.

Microwave transponders: These are used for communication between the vessel and the shore-based monitoring unit. Cybersecurity risks associated with these devices include data interception, tampering, and unauthorized access to the system. Encryption and secure communication protocols should be used to mitigate these risks.

Monitoring unit (Control room): The control room is the central hub of the vessel navigation and manoeuvring system. Security risks associated with this component include unauthorized access to the system, data breaches, and system malfunctions due to malware or other cyberthreats. Adequate cybersecurity measures should be in place, including access controls, firewalls, and a regularly updated antivirus software.

Portable Pilot's Devices (PPU): PPU devices are portable devices that pilots use to navigate and manoeuvre the vessel. They are typically connected wirelessly to the vessel's network or systems. The primary cybersecurity risk associated with PPU devices is unauthorized access or tampering of the data transmitted or stored on the device. To mitigate this risk, the PPU device should have strong authentication protocols, such as password protection, biometric authentication, or smart card authentication. In addition, data encryption should be used to protect the data transmitted wirelessly.

Laptop/Tablet (Docking Software): Laptops and tablets are often used by vessel crew to operate docking software. The primary cybersecurity risks associated with docking software on laptops or tablets are unauthorized access, data tampering, and malware infections. To mitigate these risks, proper authentication and encryption protocols should be used to protect the data transmitted or stored on the device. In addition, regular security updates and patches should be applied to the software to prevent malware infections.

Wireless transceivers: These devices are used for wireless communication between different components of the vessel navigation and maneuvering system. Cybersecurity risks associated with these devices include data interception, unauthorized access to the system, and system malfunctions due to cyberthreats. Proper encryption and secure communication protocols should be used to mitigate these risks.

Automatic Identification System: AIS is a tracking system used for vessel traffic management. The primary cybersecurity risks associated with AIS are unauthorized access, data tampering, and GPS spoofing attacks. To mitigate these risks, proper authentication and encryption protocols should be used to protect the data transmitted or stored on the device. In addition, GPS jamming or spoofing detection technologies should be implemented to prevent GPS-related attacks.

Differential GPS (DGPS): DGPS is used for accurate positioning and navigation of vessels. Cybersecurity risks associated with DGPS include data breaches, data tampering, and system malfunctions. Adequate cybersecurity measures should be in place to prevent these risks, including encryption and secure communication protocols.

Gyro compass: The gyro compass is used for navigation and positioning purposes. Cybersecurity risks associated with this component are relatively low, as it is a standalone device that is not connected to any network or system.

Electronic Chart Display and Information System (ECDIS): ECDIS is a computer-based navigation system that displays electronic navigational charts. The primary cybersecurity risks associated with ECDIS are unauthorized access, data tampering, and malware infections. To mitigate these risks, robust authentication and encryption protocols should be used to protect the data transmitted or stored on the device. In addition, regular security updates and patches should be applied to the ECDIS software to prevent malware infections.

Satellite receiver: The satellite receiver is used for communication and positioning purposes. Cybersecurity risks associated with this component include data breaches, data tampering, and unauthorized access to the system. Proper encryption and secure protocols should be used to mitigate these risks.

C. Malicious or unauthorised access to the Berthing Aid System (BAS)

Berthing Aid System (BAS) is a system used by vessels to assist in the process of berthing. BAS components can vary depending on the specific implementation and requirements. The primary cybersecurity risks associated with employee access to BAS are unauthorized access, data tampering, and data loss. The security risk assessment and mitigation strategies for this event are provided as follows:

Unauthorized Access: Unauthorized access to the BAS by an employee can result in data breaches and system damage. This could occur due to an employee accessing the system without the proper authorization or credentials. It could also result from an employee using another employee's credentials. To mitigate the risk of unauthorized access, access to the BAS should be restricted to authorized personnel only. Access should be granted based on the principle of least privilege, which means employees should only have access to the parts of the system that are necessary for their job. Strong authentication and password policies should be implemented, and regular audits of access logs should be conducted.

Data Tampering: An employee with unauthorized access to the BAS could potentially tamper with the data stored in the system. This could lead to incorrect information being displayed on the system, which could result in dangerous situations. To mitigate the risk of data tampering, data should be encrypted both in transit and at rest. Access to the system should be logged, and regular audits should be conducted to detect any unauthorized access or data tampering.

Data Loss: An employee with unauthorized access to the BAS could potentially delete or corrupt data stored in the system, leading to data loss or system failure. This could result in delays, accidents, or financial loss. To mitigate the risk of data loss, regular backups of the data stored in the system should be made. Access to the system should be restricted, and

TABLE II

SUMMARY OF THE RISK ASSESSMENT AND MITIGATION FOR THE GIVEN SCENARIOS

Scenarios	Asset	Threat	Risk	Proposed mitigations
A	Communication Systems	Spoofing, Jamming & unauthorised modifications	High	IDS (Intrusion Detection System), IPS (Intrusion Prevention System), Firewalls, encrypting communication channels (e.g. VPN, SSL)
	Navigation System	Unauthorised modification & tempering	Severe	Regular risk assessment, secure communication protocols (TLS-SSL) [16],
	OT – Tug boats	Compromised control systems (attackers)	High	Segregation of IT & OT networks, upgrading legacy systems
	Crew (employees)	Insider threat, human error, and data breach	Medium	Pre-employment checks, termination procedures, training, backup, and redundancy
B	Laser sensors, Ultrasound & Radar	Tampering and unauthorised interception of data	Low	Encryption & Secure transmission protocol
	Microwave transponders	Unauthorised access and modification of the data	High	Encryption [16] & Secure transmission protocol (TLS-SSL) [16]
	Control room	Malware, Unauthorised access, and system malfunctions	High	Firewall, anti-malware and access control, IDS and IPS
	Portable Pilot's Devices	Equipment malfunction, tampering, unauthorised access, malware	Medium	MFA, Biometric, secure passwords, encryption (TLS) [16], secure configuration, and anti-malware
	Laptop/Tablet (Docking Software):	Theft, unauthorised disclosure of information, malware, and tempering.	High	Encryption, Secure transmission protocol and patch management
	Wireless transmitter/receiver	Interception, system malfunctions and unauthorized access and jamming	High	Encryption & Secure transmission protocol
	Automatic Identification System	Spoofing, jamming, data tampering, unauthorised access and data breach	High	Encryption [16], Anti GPS jamming, access control and secure transmission protocol
	Differential GPS (DGPS):	Data breaches, data tampering and system malfunction	Medium	Encryption [16] & Secure transmission protocol
C	BAS	Unauthorized Access, Data Tampering, data breach, malware	Severe	Training, Strong authentication, secure password policies, regular audits and anti malware

only authorized personnel should have the ability to modify or delete data. Data recovery procedures should be in place in case of a system failure.

Malware Infections: Malware infections are a common risk associated with employee access to computer systems. An employee with access to the BAS could inadvertently introduce malware into the system through the use of infected devices or software. To mitigate the risk of malware infections, all devices used to access the BAS should be scanned for malware and updated regularly with the latest security patches. Antivirus software should be installed on all devices used to access the system, and employees should be trained on safe computing practices, such as avoiding clicking on suspicious links or downloading unknown software.

Social Engineering: Social engineering attacks, such as phishing and spear-phishing, are a common method of gaining unauthorized access to computer systems. An employee with access to the BAS could be tricked into providing their credentials to an attacker, leading to a data breach. To mitigate the risk of social engineering attacks, employees should receive training on how to recognize and respond to phishing attempts. Regular security awareness training should be conducted to reinforce safe computing practices. Multi-factor authentication should be implemented to reduce the risk of stolen credentials being used to gain unauthorized access to the system.

Overall, the risks associated with cybersecurity for the aforementioned scenarios are significant and can have severe consequences for the vessel, crew, and other vessels in the vicinity. To mitigate these risks, comprehensive cybersecurity risk assessments and countermeasures must be implemented to protect the vessel and the tug boat's communication, navigation, and OT systems, as well as to address the human factors that can contribute to security breaches. Table II presents a summary of the risk assessment and the mitigation strategies. The risk ratings range from low to severe. Threats with low ratings have minimal impact, while those with severe have the highest rating due to the possibility of losing human life.

IV. SIMULATION OF RADAR SPOOFING

Attacks capable of spoofing the vision of radar systems can lead to collisions without real-time warning signals and have been significantly improved over the last several years. We demonstrate a realistic attack scenario on the velocity and range of boats and vessels, which can lead to false positioning and, worse, creating copies of objects coherent with the dimension of real objects. More sophisticated attacks were also designed to follow the laws of physics of steering in water, making them harder to detect [17], [18]. Figure 1 shows the results of our simulations, where the right graph is the manipulated radar vision after a series of Frequency Modulated Continuous Wave attacks by a radar adversary. The figure on the left represents the ground truth without the attack. 12 additional copies of objects were created, while the position of one boat was moved while reliably maintaining its geometries. The highlighted rows in Table III indicate the copies of objects which, as illustrated in the table, closely match the dimensions of real objects in this scenario. These forms of attacks can mislead naval military operations or harbour management activities.

V. CONCLUSION

The maritime industry is continuously evolving and embracing digitisation to achieve operational efficiency. The interconnectivity of the fleet and the onboard technologies introduce new cyberthreats. Identifying these threats in the maritime industry significantly contributes to the safety of crews and vessels. Maritime companies will need to prepare and implement a robust cybersecurity strategy to deal with potential cybersecurity risks. In this paper, the risk assessment and mitigation strategies for three distinct cybersecurity scenarios were presented in the context of the maritime industry, to reduce the impact of possible attacks. We also demonstrated through simulating the radar spoofing attacks, the potential impact of the success of the attacks on the operation, assets

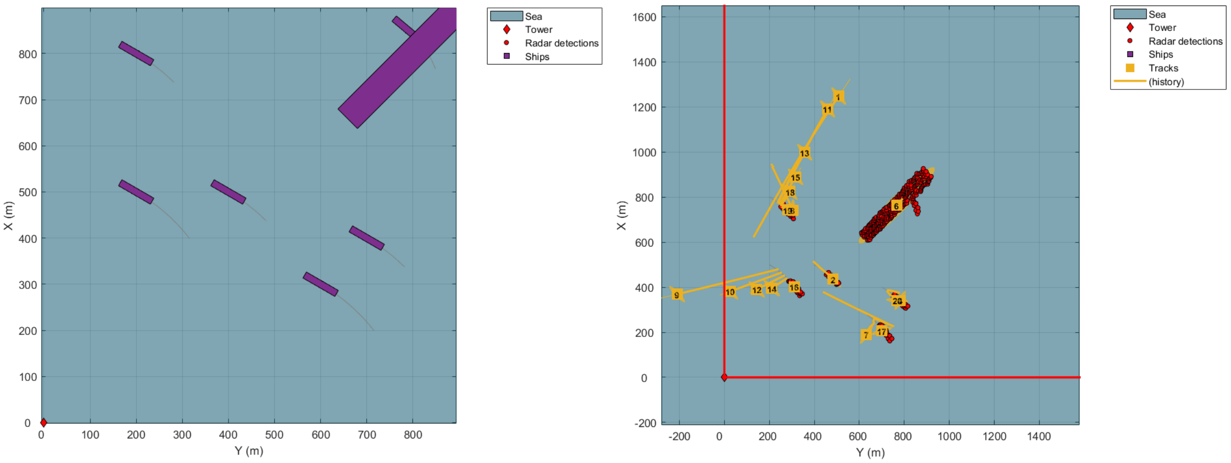

Fig. 1. (left) Ground truth harbour scenario including a vessel and a set of docking boats. (right) Radar detection while being exposed to radar spoofing activities using frequency-domain attacks.

TABLE III
RESULTS OF SPOOFING RADAR DETECTION. THE HIGHLIGHTED ROWS SHOW THE INJECTED OBJECTS THROUGH FREQUENCY MODULATION ATTACKS.

TrackID	Length	Width	Height
1	101.41	20.167	19.657
2	100.83	20.345	18.794
4	98.1	20.967	18.865
6	477.33	74.57	11.39
7	100.37	20.653	19.249
8	98.967	20.169	19.637
9	100.68	20.629	19.647
10	101.24	20.096	19.647
11	100.6	20.402	19.628
12	101.28	20.091	19.628
13	100.04	20.396	19.628
14	101.06	20.052	19.656
15	99.857	20.321	19.647
16	100.84	20.72	19.282
17	99.836	20.89	19.097
18	99.803	20.276	19.618
19	99.323	21.514	19.467
20	99.947	20.42	19.158

and personnel. We plan to expand this work in the future, incorporating risk assessment frameworks such as the ISO 27005 [19] and NIST SP800-82 Rev.3 (Draft) [20]. The framework will help maritime companies to standardise their security measures and response mechanisms to deal with potential cyber incidents.

REFERENCES

[1] M. A. Ben Farah, E. Ukwandu, H. Hindy, D. Brosset, M. Bures, I. Andonovic, and X. Bellekens, “Cyber security in the maritime industry: A systematic survey of recent advances and future trends,” *Information*, vol. 13, no. 1, p. 22, 2022.

[2] E.-C. Davri, E. Darra, I. Monogioudis, A. Grigoriadis, C. Iliou, N. Mengidis, T. Tsikrika, S. Vrochidis, A. Peratikou, H. Gibson *et al.*, “Cyber security certification programmes,” in *International Conference on Cyber Security and Resilience (CSR)*. IEEE, 2021, pp. 428–435.

[3] J. Kern, “The digital transformation of logistics: A review about technologies and their implementation status,” *The digital transformation of logistics: Demystifying impacts of the fourth industrial revolution*, pp. 361–403, 2021.

[4] E. P. Kechagias, G. Chatzistelios, G. A. Papadopoulos, and P. Apostolou, “Digital transformation of the maritime industry: A cybersecurity systemic approach,” *International Journal of Critical Infrastructure Protection*, vol. 37, p. 100526, 2022.

[5] Ö. Söner, G. Kayisoglu, P. Bolat, and K. Tam, “Cybersecurity risk assessment of vdr,” *The Journal of Navigation*, pp. 1–18, 2023.

[6] M. Afenyo and L. D. Caesar, “Maritime cybersecurity threats: Gaps and directions for future research,” *Ocean & Coastal Management*, vol. 236, p. 106493, 2023.

[7] P. Chen, Z. Zhang, Y. Huang, L. Dai, and H. Hu, “Risk assessment of marine accidents with fuzzy bayesian networks and causal analysis,” *Ocean & Coastal Management*, vol. 228, p. 106323, 2022.

[8] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, “Cybersecurity challenges in the maritime sector,” *Network*, vol. 2, no. 1, pp. 123–138, 2022.

[9] M. Lehto, “Cyber security in aviation, maritime and automotive,” *Computation and Big Data for Transport: Digital Innovations in Surface and Air Transport Systems*, pp. 19–32, 2020.

[10] R. R. Negenborn, F. Goerlandt, T. A. Johansen, P. Slaets, O. A. Valdez Banda, T. Vanelslander, and N. P. Ventikos, “Autonomous ships are on the horizon: here’s what we need to know,” *Nature*, vol. 615, no. 7950, pp. 30–33, 2023.

[11] A. Androjna, T. Brcko, I. Pavic, and H. Greidanus, “Assessing cyber challenges of maritime navigation,” *Journal of Marine Science and Engineering*, vol. 8, no. 10, p. 776, 2020.

[12] A. Goudosis and S. Katsikas, “Secure ais with identity-based authentication and encryption,” *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 14, no. 2, 2020.

[13] C. Park, C. Kontovas, Z. Yang, and C.-H. Chang, “A bn driven fmea approach to assess maritime cybersecurity risks,” *Ocean & Coastal Management*, vol. 235, p. 106480, 2023.

[14] H. M. Tusher, Z. H. Munim, T. E. Notteboom, T.-E. Kim, and S. Nazir, “Cyber security risk assessment in autonomous shipping,” *Maritime economics & logistics*, vol. 24, no. 2, pp. 208–227, 2022.

[15] B. Svilicic, J. Kamahara, M. Rooks, and Y. Yano, “Maritime cyber risk management: An experimental ship assessment,” *The Journal of Navigation*, vol. 72, no. 5, pp. 1108–1120, 2019.

[16] www.newswire.com/news/maritime-documentation-center-expands-layers-of-encryption-to-protect-20045800.

[17] R. Komissarov and A. Wool, “Spoofing attacks against vehicular fmcw radar,” in *Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security*, 2021, pp. 91–97.

[18] P. Nallabolu and C. Li, “A frequency-domain spoofing attack on fmcw radars and its mitigation technique based on a hybrid-chirp waveform,” *IEEE Transactions on Microwave Theory and Techniques*, vol. 69, no. 11, pp. 5086–5098, 2021.

[19] “Iso27005,” https://www.itgovernance.co.uk/iso27005, accessed: 2023-03-03.

[20] “Sp800-82 rev.3(draft),” https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft, accessed: 2023-03-03.