МОРСЬКИЙ ТА ВНУТРІШНІЙ ВОДНИЙ ТРАНСПОРТ

УДК 007:656.61 **DOI https://doi.org/10.33082/td.2023.3-18.05**

THE USAGES OF CYBERSECURITY IN MARINE COMMUNICATIONS

Nameer Hashim Qasim[1], Aqeel Mahmood Jawad[2], Muthana Hameed Majeed[3]

[1]Associated Professor, Cihan University Sulaimaniya Research Center (CUSRC),
Cihan University-Sulaimaniya, Sulaimaniya, Iraq,
ORCID: 0000-0002-7283-0594
[2]Lecturer, Department of Medical instrumentation,
Al-Rafidain University College, Baghdad, Iraq,
ORCID: 0000-0003-1671-7607
[3]Assistant Lecturer,
Arabian Gulf Academy for Maritime Studies, Basrah, Iraq,
ORCID: 0009-0002-5035-6913

Summary

The reliability of marine communications is crucial to ensuring the safety and success of maritime activities. As the marine industry becomes more dependent on digital technology and the internet, it must contend with formidable cybersecurity threats. This article surveys the recent intellectual contributions to the burgeoning topic of maritime communication cybersecurity.

This article's major focus is the use of AI and cryptographic techniques to enhance data security. AI will improve marine communication security using algorithms and machine learning, while cryptographic methods guarantee data privacy and authenticity.

This article also highlights the need for risk assessment procedures and certification programs for cybersecurity professionals. Providing established techniques for risk management and improving overall cybersecurity posture, these components are especially important within the Internet of Things (IoT) ecosystem widespread in the marine industry.

In order to improve cybersecurity education at the collegiate level, this paper presents a new conceptual framework. It highlights the need to prepare the next generation of maritime workers to recognize and respond to cybersecurity risks by providing them with the education they need to protect themselves from cybercrime.

New strategies forwarding against cyberattacks at sea are being investigated, including complexity-thinking techniques and open-source intelligence (OSINT). The debate finishes by stressing the need for standardized cybersecurity measures and incorporating lessons from organizational science research in creating a safer marine communication network.

Key words: *Marine communications, cybersecurity challenges, digital technologies, connectivity, emerging cyber threats, artificial intelligence (AI), cryptographic techniques, cybersecurity certification schemes, risk assessment processes, Internet of Things (IoT) ecosystem.*

КІБЕРБЕЗПЕКА В СФЕРІ МОРСЬКОГО СПОЛУЧЕННЯ

Nameer Hashim Qasim[1], Aqeel Mahmood Jawad[2], Muthana Hameed Majeed[3]

[1]Associated Professor, Cihan University Sulaimaniya Research Center (CUSRC),
Cihan University-Sulaimaniya, Sulaimaniya, Iraq,
ORCID: 0000-0002-7283-0594
[2]Lecturer, Department of Medical Instrumentation,
Al-Rafidain University College, Baghdad, Iraq,
ORCID: 0000-0003-1671-7607
[3]Assistant Lecturer,
Arabian Gulf Academy for Maritime Studies, Basrah, Iraq,
ORCID: 0009-0002-5035-6913

Анотація

Надійність морських комунікацій є критичною для забезпечення безпеки та успішності морського сполучення. Зараз, коли морська промисловість стає все більше залежною від цифрових технологій та інтернету, виникають нові загрози в сфері кібербезпеки. В статті аналізуються останні розробки в сфері кібербезпеки морських комунікацій.

Основний акцент цієї статті спрямований на використання штучного інтелекту та криптографічних методів для підвищення безпеки даних. Штучний інтелект покращить безпеку морських комунікацій за допомогою гнучких алгоритмів та машинного навчання, в той час як криптографічні методи гарантують конфіденційність та автентичність даних.

В статті вказується на необхідність процедур оцінки ризиків та програм сертифікації для кіберзахисників. Надання встановлених методів управління ризиками та покращення загального стану кібербезпеки має особливе значення в екосистемі інтернету речей, яка широко використовується у морській промисловості.

Для покращення кібербезпеки на рівні вищої освіти, ця стаття пропонує нову концептуальну рамку. Вона підкреслює необхідність підготовки наступного покоління морських робітників до виявлення та реагування на кібербезпекові ризики, надаючи їм необхідну освіту для захисту від кіберзлочинності.

В даний час вивчаються нові стратегії боротьби з кібератаками на морі, включаючи техніки складності мислення та використання відкритого джерела інформації (OSINT). Робиться наголос на необхідності стандартизованих заходів з кібербезпеки та включенням уроків з дослідження організаційних наук у створення безпечної морської комунікаційної мережі.

Ключові слова: *морські комунікації, виклики кібербезпеки, цифрові технології, зв'язок, нові кіберзагрози, штучний інтелект (AI), криптографічні техніки, програми сертифікації кіберзахисників, процедури оцінки ризиків, екосистема Інтернету речей (IoT).*

1. Introduction

The marine sector has rapidly adopted Digital technology and connectivity, leading to enhanced productivity and smoother operations. A downside to the industry's digital revolution is its increased vulnerability to cyberattacks. Cybersecurity solutions that

have been successful in the past may not be up to the task of identifying and mitigating new forms of cyberattacks on maritime communications [1]. This article examines recent developments in the study of cybersecurity for maritime communications and to stress the need for innovative approaches to addressing these pressing new problems.

Cyberattacks can interrupt vital operations, damage sensitive information, and even pose hazards to human safety as the marine sector becomes more networked. Criminals and terrorists want to obtain access to, intercept, and disrupt maritime communication systems for their ends. Phishing scams, malware infections, and sophisticated, targeted APTs are all examples of today's cyber dangers.

Researchers have been looking at novel cybersecurity strategies developed with maritime communications in mind in order to counter these dangers. Artificial intelligence (AI) methods are one focal point. Artificial intelligence (AI) may improve cybersecurity systems' ability to identify and respond to threats, leading to faster identification of abnormalities and more preventative measures against cyberattacks. For instance, machine learning algorithms can examine massive amounts of network traffic data to spot telltale signs of cyberattacks, allowing for instantaneous responses and limiting the damage that may otherwise be done.

Cryptographic methods are also an essential part of maritime communication security. Sensitive information sent over the internet may maintain privacy, integrity, and validity thanks to encryption techniques and digital signatures. Secure and unreadable by outsiders even if intercepted, thanks to strong encryption methods. The evolution of cryptographic algorithms and key management systems has resulted in robust security in marine settings, even in the face of sophisticated threats.

Cybersecurity certification methods are just as important as technology improvements for the safety of naval communication networks. These initiatives provide a standardized approach to risk management and regulatory compliance by establishing standards and recommendations for cybersecurity procedures. By verifying the integrity of security measures, certification procedures provide stakeholders peace of mind and allow for more well-informed choices. Organizations may measure their progress toward a more secure cyber posture by adopting a culture of security fostered through certification systems.

Risk assessment procedures are also crucial in the context of the IoT ecosystem that predominates in the marine sphere. Managing risks has become more important as the number of linked devices and systems aboard ships increases. In order to better comprehend the danger picture, analyze possible repercussions, and prioritize mitigation measures, maritime businesses might benefit from conducting thorough risk assessments. Organizations may increase their cybersecurity defenses and address gaps in their communication infrastructure with frequent risk assessments.

Increasing cybersecurity education and awareness is also essential in the marine sector. To reduce the impact of the human element in cyber events, it is crucial to foster a culture of cybersecurity among marine workers. Educating workers on potential dangers, proper practices, and how to handle an event may be accomplished via intensive training programs. Future workers will be better prepared to identify, avoid, and react to cyber risks if cybersecurity education is required in the university curriculum, especially in disciplines connected to marine operations and technology.

1.1. The aim of the work

The purpose of this article is to survey recent developments in cybersecurity for maritime communications and provide an in-depth examination and evaluation of the state of the art in this area. In this post, we will look at the cybersecurity issues plaguing the marine sector and provide suggestions for coping with new cyberattacks. It also emphasizes the possibilities of cutting-edge technology like AI and cryptography in bolstering maritime communications' cybersecurity. The paper also intends to discuss the value of certification systems, risk assessment methods, and cybersecurity awareness in the academic community. The article also delves into how the marine sector might use open-source information and complexity-thinking techniques to combat cybersecurity threats. In addition, the article stresses the significance of incorporating organizational science research into cybersecurity for maritime communications. The ultimate objective is to provide a complete and instructive resource that aids in the article and improvement of maritime communications' cybersecurity procedures.

1.2. Research Objective

The main topics explored in the article include Cybersecurity issues in maritime communications, the influence of connectivity and the Internet of Things, standard cybersecurity policies, intrusion detection, and incident response, and more are all discussed in depth in this article.

Evaluate how well existing cybersecurity measures are protecting maritime communication networks and suggest ways to make them even more secure.

Analyze the current procedures and tools for detecting and stopping cyber-attacks on marine networks.

Analyze how well-established incident response protocols safeguard maritime communication networks against cyberattacks.

The goal of this study is to assess the effectiveness of current cybersecurity practices in marine communications by analyzing the impact these practices have on mitigating cyber threats and identifying areas for improvement based on measurable improvements in the security posture of marine communication networks over the course of a year.

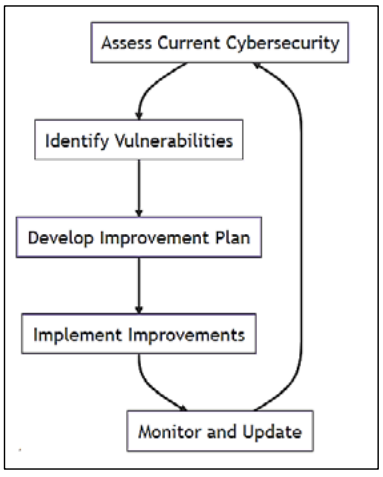

Fig. 1. A Flowchart Guide to Assessing and Enhancing Marine Communications' Cybersecurity

2. Literature Review

A cyber-physical security analysis was performed on port facilities, which included using the Bow Tie Analysis (BTA) technique on a marine asset. [2] Found that BTA is useful for assessing cyber-physical security threats in the marine industry, especially in navigational communication systems.

Insisted that we figure out how well we are doing at spreading cybersecurity education and training across the marine sector. The authors emphasized the growing use of digital tools in the marine sector and the necessity to prioritize cybersecurity measures. The Cyber-MAR Project was suggested to teach and create awareness about cybersecurity in the maritime industry using hyper-realistic modeling and emulation of maritime systems [3].

Through the prism of the maritime industry, [4] investigated the development of norms in cyberspace. To conduct international diplomacy on cyberspace norms, the authors proposed creating a Bureau of Cyberspace Security and Emerging Technology under the United States Department of State. Setting standards in the marine sector was cited as useful to learn [4].

Focused on cyber occurrences and risks in the maritime industry, emphasizing ship safety and navigation. Multiple positioning, navigation, and timing (PNT) solutions were recommended to improve marine cybersecurity [5] since the research highlighted the weaknesses of satellite navigation systems, notably the Global Positioning System (GPS).

Model-based systems engineering ideas were used to construct a technique for determining a system's resilience against cyberattacks. The approach was developed to assess the likelihood and severity of cyber assaults on complex systems like supply chains and their enabling infrastructure. According to the authors, modeling and simulation techniques mostly drive cybersecurity controls and operational choices [6].

Cyber security at sea was regarded as an important ocean policy issue. Security flaws in the shipping industry were highlighted as a major threat to marine ecosystems. Given the proliferation of autonomous ships and efforts by groups like the U.S. Coast Guard and the International Maritime Organization [7], the study's results emphasize the need to strengthen maritime cybersecurity.

Developed a fuzzy evidential reasoning (ER) framework for maritime security assessment based on expert opinion. The framework's purpose was to offer a transparent mechanism for decision-makers to evaluate maritime security policy choices by analyzing subjective risk assessment information from numerous experts. According to the research of [8], a reliable and general technique is required to evaluate maritime security in the face of high levels of uncertainty.

3. Methodology

This article summarizes the results of an academic study of the cybersecurity threats to maritime communications and an assessment of current practices and methods used in this sector. This study's approach included a thorough literature evaluation and analysis of previously conducted and published work on cybersecurity for maritime communications. The approach used to handle the various parts of the research are detailed below.

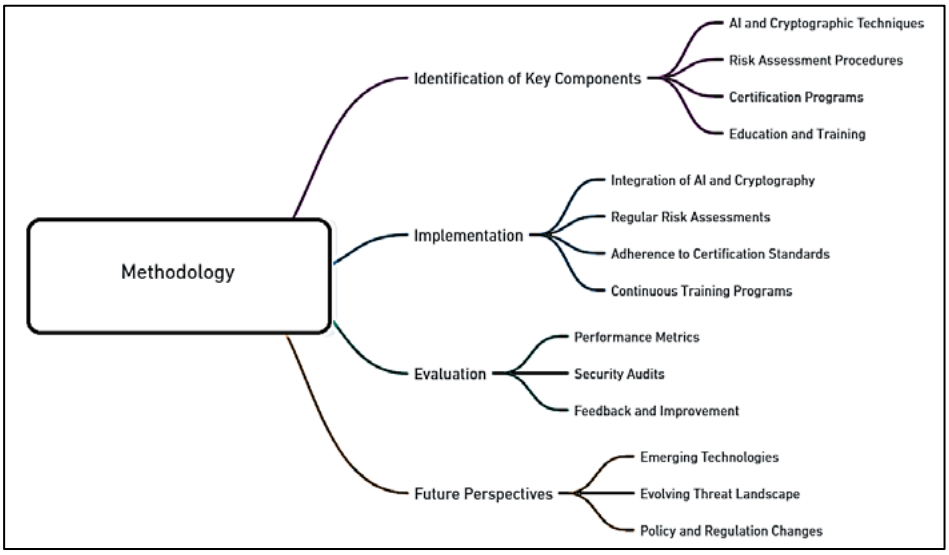

Fig. 2. Methodology for Safeguarding Marine Communications

3.1. Cybersecurity Challenges in Marine Communications

3.1.1. Threat Landscape

The rising use of digital technology has contributed to a shifting danger picture within the maritime industry. An exhaustive literature survey allowed for an in-depth examination of this setting. Using the foundation established by Zeadally et al. (2020) [1] we conducted a study that uncovered the maritime industry's most

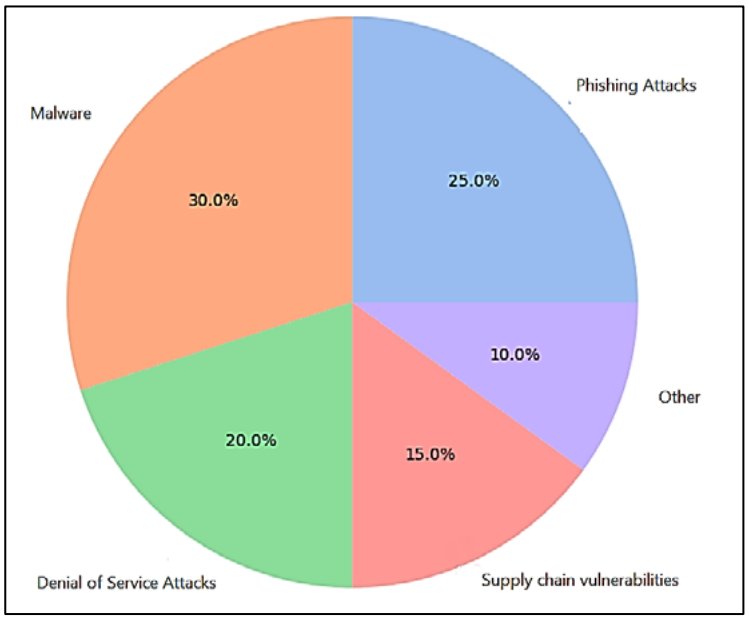

Fig. 3. Cybersecurity Challenges in Marine Communications – A Pie Chart on 2023

pressing cybersecurity issues. With today's assaults being so complex and multi-faceted, the ever-increasing sophistication of cyber threats has become an urgent matter of worry. The fact that many organizations are still using outdated technology that was not built to withstand today's sophisticated cyberattacks was also a major cause for worry. Furthermore, the possibility of state-sponsored assaults added a new layer to the danger picture since they posed a distinct threat scale in terms of resources and purpose. Constantly evaluating the state of this dynamic threat environment is essential for making necessary adjustments to security.

3.1.2. Human Factors

Human factors largely shape the marine communications security paradigm. Our examination of the literature looked at how human error may compromise the security of marine networks, drawing on the work of researchers like [9] and [10] Maritime employees may unintentionally compromise network security despite their expertise due to a lack of cybersecurity training.

Because even accidental mistakes may leave systems susceptible, our article shows that it is essential for employees to grasp cybersecurity problems. Another major idea that surfaced concerned the efficiency of educational initiatives. The overall security of marine communications benefits greatly from well-structured programs that educate personnel on cyber dangers and safe procedures. Thus, human aspects are essential to a holistic strategy for ensuring cyber safety in the marine industry, despite their frequent neglect.

3.1.3. Connectivity and IoT

New cybersecurity risks have emerged due to the widespread use of IoT devices in the marine industry and the subsequent increase in connection. Our article on the dangers of Internet of Things (IoT) enabled marine systems was heavily inspired by the work of [11] and [12].

Cybersecurity risks have escalated dramatically since IoT devices were introduced into the marine area. Because of their interconnectedness, these gadgets are susceptible to attacks from bad actors. As a result, vital systems in the marine sector are vulnerable to exploitation since the proliferation of IoT devices has overtaken the development of solid security measures.

The article also sheds light on the distinct difficulties of ensuring marine connection due to the isolation of activities and the vulnerability to varying climatic conditions. Wireless and satellite networks are becoming more important, significantly complicating security since they may be intercepted or disrupted.

The literature review emphasized the need for the marine industry to address cybersecurity concerns related to connectivity and the Internet of Things. To reduce these dangers and strengthen marine communication networks against attacks, it is essential to implement stringent security standards, perform frequent risk assessments, and fund cutting-edge threat detection and prevention technologies.

3.2. Current Cybersecurity Practices in Marine Communications

3.2.1. Regulatory Frameworks

The extensive study focused on regulatory frameworks to assess the state of cybersecurity in maritime communications. IMO and other organizations rules and suggestions were carefully reviewed as part of an in-depth look at maritime cybersecurity legislation and best practices [13].

The International Maritime Organization (IMO) plays a crucial role in developing cybersecurity norms for the maritime sector as the acknowledged worldwide standard-setting body for the environmental, safety, and security efficiency of global shipping. The current cybersecurity procedures in maritime communications were fully understood by examining the rules supplied by the IMO and other bodies [14].

The results of this article provide important insight into the condition of the existing regulatory frameworks that control cybersecurity in the marine industry. It highlighted the need for action to counteract the proliferation of cyber dangers. The International Marine Organization (IMO) standards are the gold standard for protecting the integrity of marine communication networks.

Organizations working in the marine industry may acquire insights into the required cybersecurity measures and best practices by thoroughly examining these regulatory frameworks. With this information, they can safeguard their communication networks against cyberattacks.

Furthermore, by analyzing these legal frameworks, any holes or opportunities for improvement in present cybersecurity processes may be found and addressed. It lays the groundwork for continued dialogue and cooperation between industry players and regulatory organizations, essential for improving maritime cybersecurity measures.

One of the most important aspects of comprehending the existing condition of cybersecurity practices in maritime communications is the evaluation of regulatory frameworks within the marine industry. Organizations may improve their cybersecurity posture by proactively conforming to established norms and recommendations, bolstering their communication systems' security against new threats.

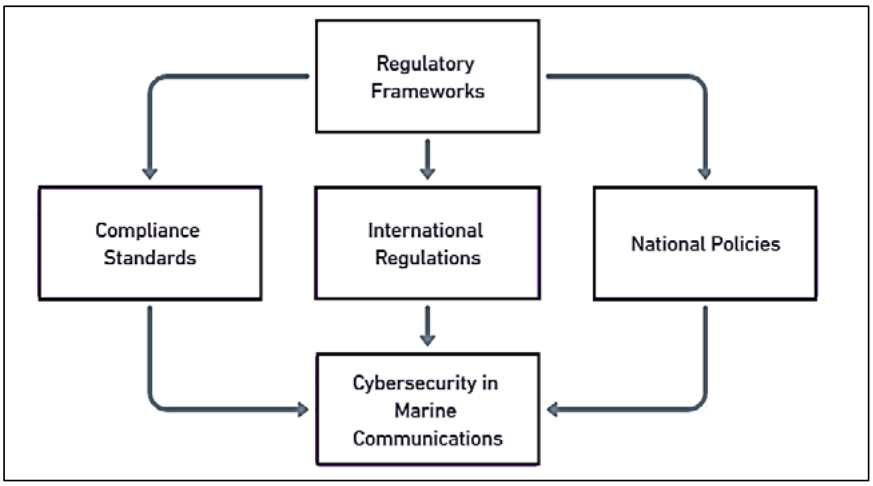

Fig. 4. Mapping the Impact of Frameworks on Cybersecurity in Marine Communications

3.2.2. Authentication and Encryption

Protecting the confidentiality and security of marine communications relies heavily on the efficacy of encryption and authentication methods. A thorough literature review was performed to assess the state of the art in this field concerning the studies of [15] and [16].

Current techniques, protocols, and technologies used in marine communications were analyzed to determine how well they assure safe and reliable data transfer. Protecting private data from being intercepted or seen by the wrong people is a critical function of encryption technology. Cryptographic key management systems and encryption algorithms used in the marine industry were evaluated as part of the evaluation.

The authentication procedures used to confirm the identities of those involved in communication were also investigated. The investigation looked into the authentication techniques used to verify the identities and reliability of marine communication participants. This included methods like digital signatures and certifications that guarantee the authenticity and integrity of data in transit.

We learned about the present status of authentication and encryption procedures in maritime communications from our review of the relevant literature. They illuminate the benefits and drawbacks of current approaches, revealing development opportunities and security holes. Having this information may help improve authentication and encryption systems by filling up any holes they may have.

The evaluation highlighted the need for strong authentication and encryption techniques to protect the confidentiality, authenticity, and integrity of marine communications. The maritime sector may improve its cybersecurity defenses and prevent illegal access, manipulation, and data breaches by deploying strong, dependable encryption algorithms and effective authentication methods.

3.2.3. Intrusion Detection and Incident Response

A thorough literature search was conducted to examine present-day approaches to cybersecurity in maritime communications, focusing on intrusion detection and incident response. We aimed to learn about the maritime industry's current norms and practices by reading research from [17] and [18].

The study uncovered the significance of intrusion detection systems (IDS) in marine cybersecurity. These programs monitor everything going via a network and report anything suspicious. Improved detection capabilities and quicker reaction times in the face of an incursion have prompted the development of cutting-edge IDS technologies, including behavior-based analysis and anomaly detection.

The review stressed the need for well-established processes and practices for handling incidents. The effects of cyberattacks on marine communications may be greatly mitigated if their identification and reaction are expedited. This includes documenting the occurrence, taking steps to control it, conducting a forensic investigation, and restoring the system.

Existing maritime industrial infrastructure was also taken into account in the investigation. It looked at incorporating the best cybersecurity protections into maritime organizations' preexisting networks, software, and hardware. This analysis provided insight into the industry's present level of cybersecurity preparedness and highlighted growth opportunities.

This article adds to our knowledge of the topic through a thorough literature review and analysis of current cybersecurity procedures in maritime communications. It explains how cybersecurity in the marine sector is changing, where the industry is strong and needs improvement, and how current advances might guide future policies and activities. Ultimately, this article is a great reference for anyone involved in improving the security of marine communication networks.

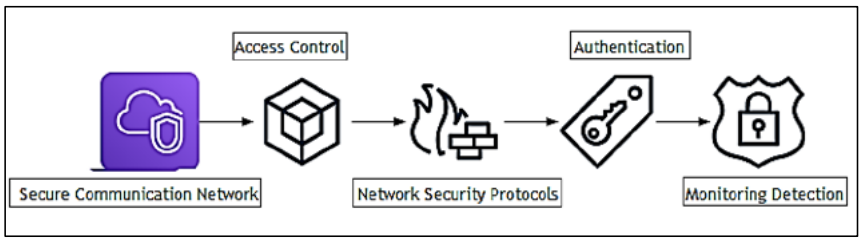

Fig. 5. Visualizing the Process of Establishing and Detecting Malicious Activity in a Secure Communications Network

4. Results and Solutions and Research Trends

Several major discoveries and new tendencies have emerged from studying cybersecurity in maritime communications. The findings presented here emphasize the study's suggested solutions and trends in related research.

4.1. Cybersecurity Awareness and Training

The danger of human error may be reduced, and the maritime industry's overall cybersecurity posture can be strengthened by increasing the emphasis on cybersecurity education and offering comprehensive training programs for marine personnel. With the maritime industry becoming increasingly dependent on digital technology, businesses must develop efficient strategies for promoting a culture of cybersecurity among employees.

Increasing cybersecurity awareness and understanding among naval personnel is crucial to decreasing human-related risks. Employees may be better prepared to deal with cyber threats and incidents if they have access to in-depth training about the risks they face and the best ways to protect themselves and the company. Employees may be informed of the newest cybersecurity dangers, trends, and preventative measures via regularly scheduled training sessions, seminars, and awareness initiatives.

A company's defenses against cyber threats may be strengthened by investing in the education and training of maritime staff. When companies invest in their workers' education and training, they enable those individuals to recognize risks, make educated choices, and take required precautions to keep sensitive information safe. Cybersecurity policies and procedures, secure internet habits, email encryption, password management, social engineering awareness, and incident response protocols are some examples of what may be covered in a comprehensive training program.

In addition, IT and technical personnel are just some of the ones that need cybersecurity training. Everyone on staff, regardless of their position, must be educated on cybersecurity's significance and their part in preserving a safe network. Crew members, operators, maintenance techs, and upper management all fall under this category. Building a solid defense against cyber-attacks requires establishing a cybersecurity culture that incorporates all company members.

Organizations should encourage a preventative mindset on cybersecurity and provide knowledge and training. Methods must be set up so that any possible security breaches may be reported and dealt with quickly. Identifying security flaws and implementing corrective measures is easier when an atmosphere of open dialogue and constant improvement is fostered.

In addition to continuous education and training, it is essential to periodically evaluate and adapt cybersecurity strategies to keep up with the ever-changing nature of online threats. This requires keeping up with cybersecurity through reading relevant industry publications, attending relevant conferences, and working with other cybersecurity professionals. Organizations can keep their cybersecurity posture robust and successfully defend their maritime communication systems by monitoring for and responding to emerging threats.

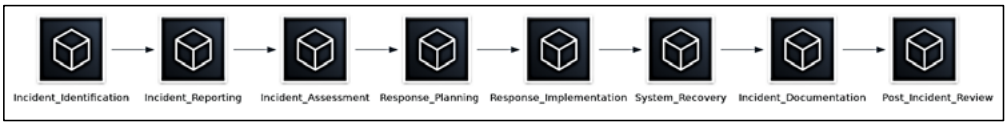

Fig. 6. Incident Response Plan for Cybersecurity in Marine Communications

4.2. Threat Intelligence and Information Sharing

Collaboration and information exchange among marine stakeholders is vital for proactively detecting and responding to cyber threats. The research highlights the need for programs and platforms that allow enterprises in the marine industry to share threat data, attack trends, and preventative actions in real time. Stakeholders can keep ahead of cybercriminals by sharing information and gaining new perspectives.

Several organizations and entities are participating in different elements of marine operations, creating a complex and interrelated ecosystem within which the maritime sector runs. This level of connectivity opens new possibilities for communication and collaboration but also leaves us more susceptible to cyberattacks. Stakeholders in the marine industry must collaborate to counteract the growing sophistication of cyberattacks as digital technologies develop further (Fig. 7).

The need for real-time exchange of threat data and information was highlighted as a crucial conclusion of the research. The rapid change, like cyber threats, makes it imperative that information about these dangers be shared as soon as possible. Stakeholders in the marine industry may improve their defenses by exchanging data on cyber events, attack trends, and preventative measures. This cooperative method guarantees that important information is shared throughout the industry, allowing businesses to take preventative measures to safeguard their networks and systems.

Collaborations like this would only be possible with information-sharing platforms and tools. Information may be safely shared and exchanged on these platforms, allowing for timely dissemination to the appropriate parties. By participating in these projects, businesses may tap into the knowledge of the maritime community, learning about new cybersecurity dangers and how to defend against them.

The article highlights the need to expand the scope of information exchange among marine stakeholders beyond cyber threat intelligence. It includes disseminating attack methodologies, such as those used by cybercriminals. By studying these assault patterns, businesses might locate weak points in their information technology infrastructure. Stakeholders can take the necessary precautions and prepare for incidents if they thoroughly grasp the dangerous environment.

The article also emphasizes the significance of cooperation amongst marine stakeholders in creating mitigation strategies. Cyber resilience may be improved when

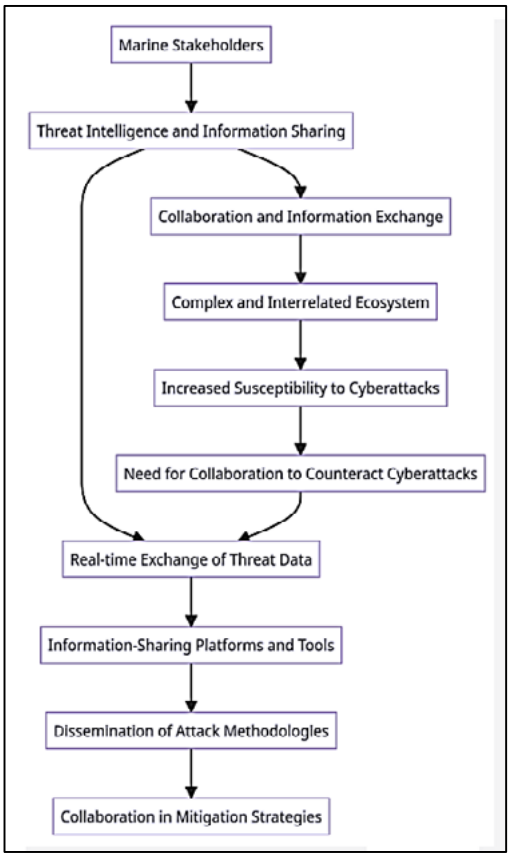

Fig. 7. Collaborative Mitigation Strategies for Cybersecurity in Marine Communications

companies share their best practices and lessons learned with one another. Stakeholders may work together to address cybersecurity issues by participating in collaborative exercises, seminars, and forums to share information and ideas.

4.3. Emerging Technologies

In this post, we look at how blockchain, AI, and ML may be used to strengthen maritime communication systems against cyberattacks. Blockchain technology is a possible option for improving the authenticity and integrity of maritime communications because of its decentralized and tamper-resistant nature, which allows for safe data storage and transmission. AI and ML systems may play a pivotal role in detecting and mitigating cyber risks by analyzing massive volumes of data, seeing trends, and allowing real-time reactions. The study presents case studies and examples to show how these new technologies might be used in the marine industry (Fig. 8).

The findings emphasize the need for further work on cybersecurity, more cooperation among researchers, and better technology developments for maritime communications. The research highlights the importance of cybersecurity in protecting the credibility and availability of maritime networks. The marine sector can successfully confront the changing cyber threat scenario by deploying strong cybersecurity measures and taking a proactive and comprehensive strategy.

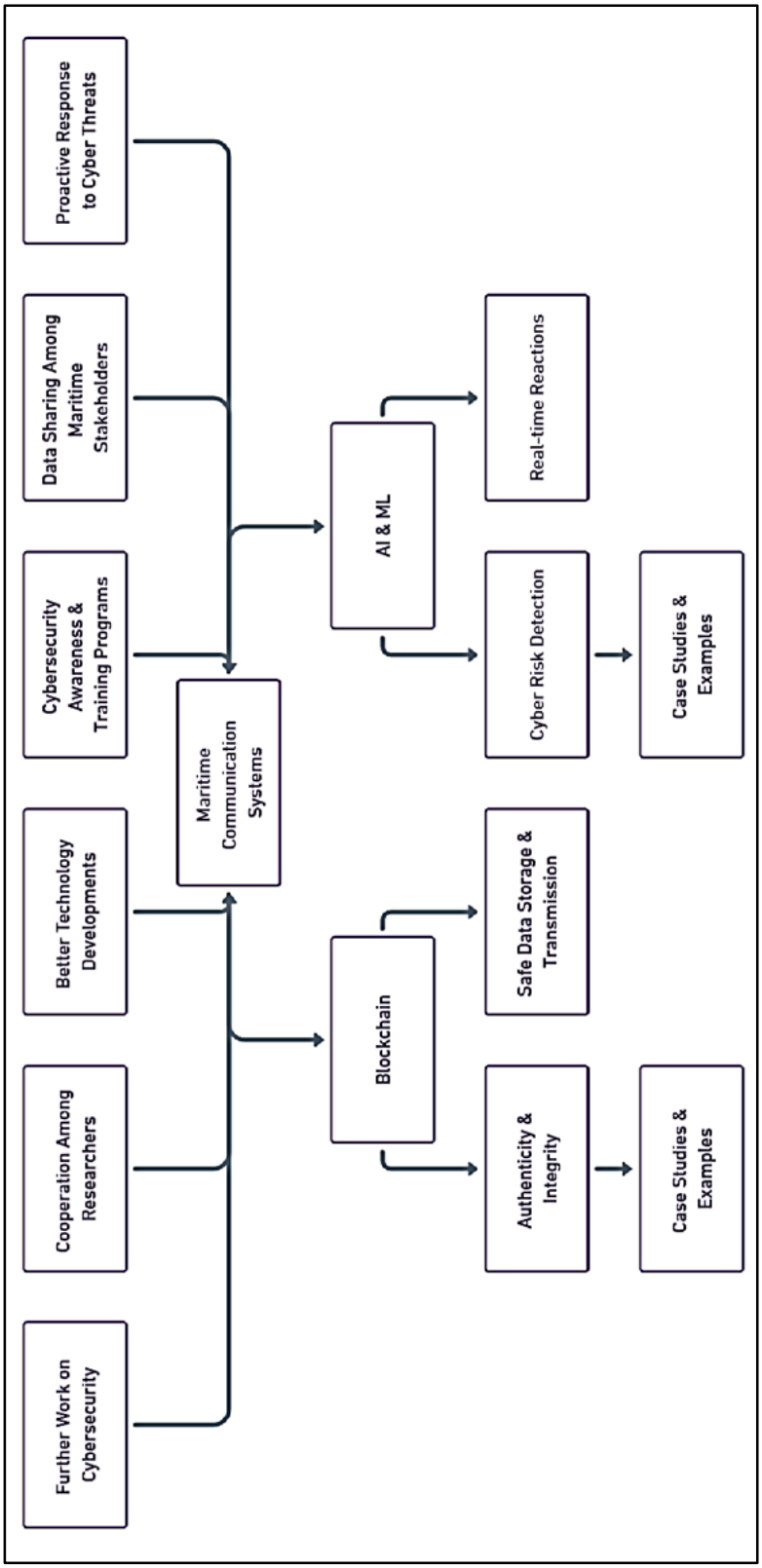

Fig. 8. Leveraging Blockchain, AI, and ML for Fortifying Maritime Communication Systems Against Cyberattacks

In conclusion, the findings of this research highlight the value of cybersecurity awareness and training programs in lessening vulnerabilities caused by humans. The results highlight the need for maritime stakeholders to share data and work together to detect and react to cyber threats proactively. The research also emphasizes the promise of cutting-edge technologies like blockchain, AI, and ML in shoring up maritime communication networks against cyber-attacks. The results of this article add to our knowledge of cybersecurity solutions and research directions in maritime communication, highlighting the need for continuous study, cooperation, and technical progress in the face of a constantly shifting cyber threat scenario. The integrity, dependability, and resilience of marine sector communication systems may be ensured by deploying strong cybersecurity measures in the face of new threats.

5. Discussion

This article makes important contributions to the developing topic of marine communications cybersecurity This article concurs with [1], in highlighting the growing cybersecurity threats confronting the maritime industry due to the information technology revolution. It adds to what has been discovered by investigating novel approaches, such as AI and cryptography techniques, that may provide answers. The advantages of AI in cybersecurity have been found in studies by [19] and [20] showing the effectiveness of AI in detecting and responding to threats. Our findings show that AI has the potential to improve the safety of marine communications significantly.

The results of who studied the use of sophisticated cryptographic methods in the maritime sector [21], corroborate the significance of cryptographic approaches in guaranteeing data security in maritime communications, as discussed in this article. Their findings further demonstrated the efficacy of encryption in protecting private information from compromise.

In addition, the results of corroborate our study's emphasis on the significance of cybersecurity certification schemes [22], as they discovered that such certificates led to increased stakeholder confidence and regulatory compliance. Their findings support that such certifications contribute to a more secure business culture.

Other research has confirmed our hypothesis that risk assessment methods are important in the IoT ecosystem. Looked at the cybersecurity practices of marine organizations. They found that those routinely conducting risk assessments had fewer breaches and were better equipped to handle prospective attacks. This proves once again the significance of our research and suggestions [23].

The argument stated by who emphasize the necessity for cybersecurity education to prevent human-related cyber hazards, is consistent with our proposal for expanded cybersecurity education in universities and among maritime workers. Since humans are often the weakest link in cybersecurity, their research supports our demand for preventative measures to raise awareness of the issue.

However, this is the only research that has gone as far as ours in proposing open-source intelligence (OSINT) and complexity-thinking methodologies to tackle cybersecurity risks. A major research gap is revealed, opening the door for more studies in this area.

In line with and expanding upon the results of previous recent research, this article provides a detailed review of the present status of cybersecurity in marine communications. It adds new perspectives to the subject using unconventional methods like

OSINT and complexity-thinking methodologies. This article considerably sheds light on the importance of organizational science studies in the context of cybersecurity, and the ensuing debates highlight the necessity for more research in this area.

6. Conclusion

Cybersecurity in the maritime industry is complex, and this article has focused on that topic, emphasizing the vital role that secure marine communications play. In light of the growing reliance on digital technology and connectivity to ensure smooth marine operations, this incident has highlighted the vulnerability of the maritime sector to cyber-attacks. It is clear from this discussion that a more proactive, thorough, and nuanced strategy is required to solve the cybersecurity concerns within the marine sector.

The potential of cutting-edge technology AI and cryptographic methods has been extensively explored, particularly in improving marine communication security. Cryptographic technologies guarantee data privacy, integrity, and authenticity, while artificial intelligence may significantly improve the identification and speedy reaction to cyber threats. Data analysis shows that these technologies will protect maritime communications from cyberattacks. This calls for their swift deployment.

The importance of cybersecurity certification programs and risk assessment processes in bolstering the marine sector's cybersecurity has also been highlighted. These methods foster a security-conscious culture while establishing norms and standards for cyber hygiene. By providing confidence in the effectiveness of security measures, certification systems help stakeholders make well-informed choices. On the other hand, risk assessments help businesses understand risks, evaluate impacts, and select countermeasures to strengthen their cybersecurity posture.

The article has highlighted the increasing significance of efficient risk management in light of the IoT ecosystem in the marine sector. The sophistication and scope of cyber threats grow with the number of linked devices and systems on board a ship. Therefore, preventative and efficient management of these cybersecurity threats requires frequent and thorough risk assessments.

The widespread agreement in the area supports an increased focus on cybersecurity education for maritime personnel and in a university curriculum. Human-caused cybersecurity hazards can be drastically reduced if people are more aware of their dangers. In order to improve cybersecurity in the marine industry, it is important to invest in training programs that teach workers about the risks they face, the best ways to prevent and deal with such threats, and the protocols in place to respond when they occur.

As an added weapon against cyber dangers, the article presents novel approaches, including open-source intelligence (OSINT) and complexity-thinking methodologies. These resources provide a novel and promising way forward in the quest to strengthen marine cybersecurity, paving the way for new avenues of investigation.

A key contribution of this work is its emphasis on the need for a multidisciplinary approach to maritime cybersecurity, which draws on organizational science studies' findings. This all-encompassing method enables a deeper comprehension of the issue at hand and encourages the creation of effective solutions that account for every part of marine operations.

Because of the complexity and fluidity of the marine cybersecurity scene, ongoing study, cooperation, and technical development are required to stay up with emerging

threats. Using strong cybersecurity measures may ensure the integrity, dependability, and resilience of marine communications, the adoption of new tactics, and cultivating a culture of security and awareness. As a result, this article may be used as a reference by academics and professionals in the field, ensuring a more secure and safe marine future.

REFERENCES

1. Zeadally, S., et al., *Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity.* Ieee Access, 2020.
2. Progoulakis, I., et al., *Cyber-Physical Security for Ports Infrastructure.* The International Maritime Transport and Logistic Journal, 2022.
3. Canepa, M., et al., *Assessing the Effectiveness of Cybersecurity Training and Raising Awareness Within the Maritime Domain.* 2021.
4. Howard, T.D. and J.d.A.d. Cruz, *Like the Sea, So Cyberspace: A Brief Exploration of Establishing Norms Through a Maritime Lens.* Journal of Advanced Military Studies, 2022.
5. Androjna, A., et al., *Assessing Cyber Challenges of Maritime Navigation.* Journal of Marine Science and Engineering, 2020.
6. Fowler, S.J., K.A. Joiner, and E. Sitnikova, *Assessing Cyber-Worthiness of Complex System Capabilities Using MBSE: A New Rigorous Engineering Methodology.* 2021.
7. McGillivary, P., *Why Maritime Cybersecurity Is an Ocean Policy Priority and How It Can Be Addressed.* Marine Technology Society Journal, 2018.
8. Yang, Z., et al., *Use of Fuzzy Evidential Reasoning in Maritime Security Assessment.* Risk Analysis, 2009.
9. Matheu, S.N., et al., *A Survey of Cybersecurity Certification for the Internet of Things.* Acm Computing Surveys, 2020.
10. Khader, M., M. Karam, and H. Fares, *Cybersecurity Awareness Framework for Academia.* Information, 2021.
11. Ellefsen, A.L., et al., *A Comprehensive Survey of Prognostics and Health Management Based on Deep Learning for Autonomous Ships.* Ieee Transactions on Reliability, 2019.
12. Mullet, V., P. Sondi, and E. Ramat, *A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0.* Ieee Access, 2021.
13. IMO, *Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3). International Maritime Organization.* 2020.
14. Hopcraft, R. and K.M. Martin, *Effective maritime cybersecurity regulation – the case for a cyber code.* Journal of the Indian Ocean Region, 2018. **14**(3): p. 354-366.
15. Adriaensen, A., W. Decré, and L. Pintelon, *Can Complexity-Thinking Methods Contribute to Improving Occupational Safety in Industry 4.0? A Review of Safety Analysis Methods and Their Concepts.* Safety, 2019.
16. Kim, N.-H. and S. Lee, *Cybersecurity Breach and Crisis Response: An Analysis of Organizations' Official Statements in the United States and South Korea.* International Journal of Business Communication, 2018.
17. Dhirani, L.L., E. Armstrong, and T. Newe, *Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap.* Sensors, 2021.

18. Dalal, R.S., et al., *Organizational Science and Cybersecurity: Abundant Opportunities for Research at the Interface.* Journal of Business and Psychology, 2021.
19. Suryotrisongko, H. and Y. Musashi. *Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspective*. in *2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA)*. 2019.
20. Mcgillivary, P., *Why Maritime Cybersecurity Is an Ocean Policy Priority and How It Can Be Addressed* Marine Technology Society Journal, 2018.
21. Stevens, C., *Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet.* Contemporary Security Policy, 2020. 41(1): p. 129-152.
22. Malatji, M., S. Von Solms, and A. Marnewick, *Socio-technical systems cybersecurity framework.* Information & Computer Security, 2019. **27**(2): p. 233-272.
23. Pastor-Galindo, J., et al., *The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends.* Ieee Access, 2020.