Güvenlik Bilimleri Dergisi / Journal of Security Sciences

Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Bilimleri Dergisi, Kolluk Uygulamaları ve Güvenlik Teknolojileri Özel Sayısı, 258-287
doi: 10.28956/gbd.1632891

Gendarmerie and Coast Guard Academy
Institute of Security Sciences
Journal of Security Sciences, Thematic Issue on Policing Practices and Security Technologies 258-287
Doi: 10.28956/gbd.1632891

Makale Türü ve Başlığı / Article Type and Title

Araştırma / Research Article

Cybersecurity and Privacy in Maritime Security: Theories, Challenges, Case Studies and Future Prospects

Deniz Güvenliğinde Siber Güvenlik ve Gizlilik: Teoriler, Zorluklar, Vaka Çalışmaları ve Gelecek Beklentileri

Yazar(lar) / Writer(s)

Alperen ERDOĞAN, Dr., Turkish National Defence University, alperen.erdogan.1985@gmail.com, ORCID: 0000-0002-4986-0904
Nuray Söğünmez ERDOĞAN, Dr., Kadir Has University - Moleküler Biyoloji ve Genetik Bölümü, nuray.sogunmez@gmail.com, ORCID: 0000-0003-0909-064X

Bilgilendirme / Acknowledgement:

-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.
-Bu makalede araştırma ve yayın etiğine uyulmuştur.
Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received : 29.04.2025
Makale Kabul Tarihi / Accepted : 09.10.2025

Atıf Bilgisi / Citation:

Erdoğan A, ve Erdoğan Sögünmez N, (2025). Cybersecurity And Privacy In Maritime Security: Theories, Challenges, Case Studies And Future Prospects *Güvenlik Bilimleri Dergisi, Kolluk Uygulamaları ve Güvenlik Teknolojileri Özel Sayısı, ss 258-287. doi: 10.28956/gbd.1632891*

CYBERSECURITY AND PRIVACY IN MARITIME SECURITY: THEORIES, CHALLENGES, CASE STUDIES AND FUTURE PROSPECTS

Abstract

The maritime domain plays a significant role in global trade, transportation, and security. However, with the increasing integration of digital technologies into maritime operations, cybersecurity and privacy have appeared as crucial concerns. This research article explores the theories underpinning cybersecurity and privacy in the maritime domain, identifies key challenges, and discusses future prospects for addressing these issues. Using a qualitative research methodology, existing literature, case studies, and technological advancements to provide insights into the current state of maritime cybersecurity have been analyzed. Scientific databases (Web of Science, Scopus, EBSCO, Google Scholar, DOAJ, and TR Dizin), books, reports, and bulletins have been main research areas. The topics, titles, abstracts, and keywords including "cybersecurity", "cyber", "security", "maritime security", "marine security", and "privacy" have been analyzed. Most read, downloaded and cited documents and papers have been researched, analyzed, and studied. Case studies have been also observed and included in the article. Our findings highlight the need for robust frameworks, international collaboration, and advanced technologies to mitigate risks and ensure secure and private maritime operations.

Keywords : *Cybersecurity, Privacy, Maritime, Marine, Security*.

DENİZ GÜVENLİĞİNDE SİBER GÜVENLİK VE GİZLİLİK: TEORİLER, ZORLUKLAR, VAKA ÇALIŞMALARI VE GELECEK BEKLENTİLERİ

Öz

Denizcilik alanı küresel ticaret, ulaşım ve güvenlikte önemli bir rol oynamaktadır. Ancak dijital teknolojilerin denizcilik operasyonlarına giderek daha fazla entegre olmasıyla birlikte siber güvenlik ve gizlilik önemli endişeler olarak ortaya çıkmıştır. Bu araştırma makalesi, denizcilik alanında siber güvenlik ve gizliliğin altında yatan teorileri incelemekte, temel zorlukları belirlemekte ve bu sorunların ele alınmasına yönelik gelecekteki beklentileri tartışmaktadır. Nitel araştırma metodolojisi kullanılarak mevcut literatür, vaka çalışmaları ve teknolojik gelişmeler analiz edilerek denizcilikte siber güvenliğin güncel durumu hakkında fikir edinilmiştir. Bilimsel veri tabanları (Web of Science, Scopus, EBSCO, Google Scholar, DOAJ ve TR Dizin), kitaplar, raporlar ve bültenler başlıca araştırma alanları olmuştur. "Siber güvenlik", "siber", "güvenlik", "denizcilik güvenliği", "deniz bilimleri güvenliği" ve "gizlilik" gibi konular, başlıklar, özetler ve anahtar kelimeler analiz edilmiştir. En çok okunan, indirilen ve atıfta bulunulan dokümanlar ve makaleler araştırılmış, analiz edilmiş ve incelenmiştir. Bu makalede vaka çalışmaları da gözlemlenmiş ve çalışmaya dahil edilmiştir. Bulgularımız; riskleri azaltmaya, güvenli ve özel denizcilik operasyonlarını sağlamak için gerçek çerçevelere, uluslararası işbirliklerine ve gelişmiş teknolojilere olan ihtiyacı vurgulamaktadır.

Anahtar Kelimeler: *Siber Güvenlik, Gizlilik, Denizcilik, Deniz Bilimleri, Güvenlik.*

INTRODUCTION

The maritime industry is a keystone of global commerce, accounting for over 80% of world trade (Kanwal et al., 2024). With the advent of digitalization, the sector has embraced technologies such as the Internet of Things (IoT), artificial intelligence (AI), and autonomous systems to enhance efficiency and safety (Kanwal et al., 2024). However, this reliance on interconnected systems has introduced vulnerabilities that malicious actors can exploit. Cyberattacks on maritime infrastructure, such as ports, vessels, and supply chains, pose significant threats to national security, economic stability, and individual privacy (Afenyo and Caesar, 2023).

This article aims to address the growing concerns surrounding cybersecurity and privacy in the maritime domain. By examining relevant theories, identifying challenges, and exploring future prospects, we seek to contribute to the development of comprehensive strategies to defend maritime operations.

Importance of the Maritime Domain

The maritime domain encompasses activities related to shipping, port operations, offshore energy production, and naval defense (Kechagias et al., 2022). These activities are vital for global economic growth, energy security, and geopolitical stability. For example, container ships transport billions of dollars' worth of goods annually, while offshore platforms produce a significant portion of the world's oil and gas. Any disruption in these operations due to cyberattacks could have flooding effects on economies and societies.

Maritime infrastructure is also an important component of national security (Akdag et al., 2022). Ports serve as gateways for military logistics, and offshore installations are often strategic assets (Khandker et al., 2022). A cyberattack on these systems could compromise national defense capabilities and disrupt global supply chains. For instance, the 2017 NotPetya ransomware attack on Maersk caused widespread operational disruptions, resulting in losses exceeding $300 million and highlighting the vulnerability of maritime systems to cyber threats.

Ports, as hubs of the global trade, are particularly susceptible to cyberattacks (Park et al., 2023). They rely on interconnected systems for cargo handling, customs clearance, and logistics management. A breach in any of these systems can lead to delays, financial losses, and reputational damage. Similarly, offshore energy platforms, which are significant for energy production, are vulnerable to

attacks that could disrupt energy supplies or cause environmental disasters (Tedeschi et al., 2022).

The maritime domain is also increasingly reliant on satellite communications and navigation systems, such as GPS, which are indispensable for vessel tracking and safe navigation (Wang, 2024). However, these systems are susceptible to jamming, spoofing, and other forms of interference. For example, GPS spoofing attacks can mislead vessels, causing them to deviate from their intended routes and potentially leading to collisions or groundings.

The Digital Transformation of Maritime Operations

Digital transformation has revolutionized maritime operations by introducing automation, real-time monitoring, and data-driven decision-making (Wang, 2024). For instance, smart ports use IoT sensors to optimize cargo handling, while autonomous ships rely on AI algorithms for navigation. While these innovations improve efficiency, they also create new attack vectors for cybercriminals. A crack in a single system can compromise an entire network, leading to operational downtime, financial losses, and reputational damage (Chaal et al., 2023).

For example, the integration of IoT devices in maritime operations allows for real-time tracking of cargo and vessel performance. However, these devices often lack robust security features, making them prone to exploitation. Similarly, autonomous ships, while reducing labor costs, rely heavily on software that can be hacked, potentially leading to catastrophic accidents or unauthorized access to sensitive data (Durlik et al., 2024).

Additionally, the maritime industry increasingly relies on cloud computing for data storage and processing (Jovic et al., 2022). While cloud solutions offer scalability and cost savings, they also introduce risks such as unauthorized access, data breaches, and service outages (Kanwal et al., 2024). Ensuring the security of cloud-based systems is therefore a critical priority for maritime organizations.

The adoption of digital twins—virtual replicas of physical assets—is another emerging trend in the maritime sector (Afenyo and Caesar, 2023). Digital twins enable predictive maintenance, optimize fuel consumption, and enhance operational efficiency. However, they also increase the attack surface, as attackers could manipulate the virtual models to disorganize real-world operations.

In addition to IoT and AI, blockchain technology is being explored for its potential to enhance transparency and trust in maritime supply chains (Park et al.,

2023). Blockchain can be used to track the provenance of goods, verify transactions, and automate processes through smart contracts. However, implementing blockchain solutions requires cautious consideration of security and privacy implications, as well as interoperability with existing systems.

1. METHODOLOGY

This study employs a qualitative research approach, combining a systematic review of academic literature, industry reports, and case studies. Data were collected from peer-reviewed journals, government publications, and maritime cybersecurity frameworks. The analysis focuses on identifying theoretical foundations, evaluating present challenges, and proposing actionable recommendations for the future.

So, this research article explores the theories underpinning cybersecurity and privacy in the maritime domain, identifies key challenges, and discusses future prospects for addressing these issues. Using a qualitative research methodology, existing literature, case studies, and technological advancements to provide insights into the current state of maritime cybersecurity have been analyzed. Scientific databases (Web of Science, Scopus, EBSCO, Google Scholar, DOAS, and TR Dizin), books, reports, and bulletins have been main research areas. The topics, titles, abstracts, and keywords including "cybersecurity", "cyber", "security", "maritime security", "marine security", and "privacy" have been analyzed. Most read, downloaded and cited documents and papers have been researched, analyzed, and studied. Case studies have been also observed and included in the article.

1.1. Data Collection

Data collection involved reviewing documents from organizations such as the International Maritime Organization (IMO) and the United Nations Conference on Trade and Development (UNCTAD). Case studies of notable cyber incidents, such as the NotPetya ransomware attack on Maersk in 2017 and the 2021 Colonial Pipeline ransomware attack, were analyzed to understand their impact and implications.

The NotPetya attack, for example, demonstrated how a single malware infection could spread across an organization's global network, crippling operations, and causing financial losses. Similarly, the Colonial Pipeline incident

highlighted the vulnerability of critical infrastructure to ransomware attacks, underscoring the significance of proactive cybersecurity measures.

In addition to these high-profile incidents, smaller-scale attacks on maritime systems have become increasingly common. For instance, phishing campaigns targeting crew members and shore-based staff have led to unauthorized access to sensitive systems. These facts highlight the need for comprehensive cybersecurity strategies that address both technical and human factors.

1.2. Limitations

While this study provides valuable insights, it is limited by the availability of primary data and the swiftly evolving nature of cybersecurity threats. Future research should incorporate quantitative methods, such as surveys and simulations, to measure the effectiveness of proposed solutions and assess the financial impact of cyberattacks on the maritime industry.

Additionally, the study's focus on qualitative data means that some findings may be subjective and open to interpretation. To address this limitation, future research should direct to triangulate findings using multiple data sources and methodologies.

2. THEORIES AND EXPLANATIONS

In the maritime domain several theories and explanations can be made in line with maritime cybersecurity. These can be grouped as cybersecurity frameworks, privacy models, game theory and cybersecurity, and systems theory.

2.1. Cybersecurity Frameworks

Several frameworks as shown in Table-1 guide cybersecurity practices in the maritime domain. These frameworks are explained in detail below :

Table-1 : Cybersecurity Frameworks

No	Framework
1	International Maritime Organization (IMO) Guidelines
2	NIST Cybersecurity Framework
3	ISO/IEC 27001

2.1.1. International Maritime Organization (IMO) Guidelines

In 2017, the IMO issued guidelines for maritime cyber risk management, emphasizing the need for a risk-based approach (Kanwal et al., 2024). These guidelines recommend identifying assets, assessing vulnerabilities, and implementing protective measures. They also encourage continuous monitoring and improvement of cybersecurity practices. The IMO framework is particularly valuable for its focus on integrating cybersecurity into the larger safety management systems of maritime organizations.

2.1.2. NIST Cybersecurity Framework

Developed by the National Institute of Standards and Technology, this framework provides a flexible structure for managing cybersecurity risks (Afenyo and Caesar, 2023). It includes five core functions: Identify, Protect, Detect, Respond, and Recover. The NIST framework is widely adopted across industries and serves as a foundation for developing tailored cybersecurity strategies in the maritime sector. Its emphasis on continuous improvement adjusts well with the dynamic nature of cyber threats.

2.1.3. ISO/IEC 27001

This international standard specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) (Park et al., 2023). ISO/IEC 27001 is particularly relevant for maritime organizations seeking to align their cybersecurity practices with global best practices. Certification to this standard can enhance an organization's credibility and shows its commitment to cybersecurity.

2.2. Privacy Models

Privacy in the maritime domain is governed by principles such as data minimization, consent, and transparency (Wang, 2024). Regulations like GDPR set benchmarks for protecting personal data, particularly for crew members and passengers. GDPR mandates that organizations implement technical and organizational measures to safeguard personal data and report breaches within 72 hours. Compliance with such regulations is significant for maintaining trust and

avoiding legal penalties.

In addition to GDPR, other privacy frameworks, such as the California Consumer Privacy Act (CCPA) and the Personal Information Protection Law (PIPL) in China, impose similar requirements on organizations operating in those jurisdictions (Park et al., 2023). Maritime companies must navigate this complex regulatory landscape to secure compliance and protect sensitive data.

2.3. Game Theory and Cybersecurity

Game theory provides a useful lens for understanding interactions between attackers and defenders in the maritime cybersecurity landscape (Berghout et al., 2022). By modeling potential attack scenarios, stakeholders can develop proactive defense strategies. For example, a "zero-sum game" model assumes that any gain by an attacker results in an equal loss for the defender, highlighting the significance of resource allocation and strategic planning.

Game theory can also help explain the behavior of state-sponsored actors, who may engage in cyber espionage or sabotage to achieve geopolitical objectives (Durlik et al., 2024). Understanding these dynamics is notable for developing effective deterrence strategies and fostering international cooperation.

2.4. Systems Theory

Systems theory views maritime operations as interconnected systems where a failure in one component can affect the entire network (Qiao et al., 2025). This perspective underscores the need for holistic cybersecurity strategies that consider both technical and human factors. For instance, a cyberattack on a port's cargo management system could disrupt shipping schedules, delay deliveries, and shock downstream supply chains.

Systems theory also emphasizes the importance of resilience, which refers to an organization’s ability to withstand and recover from cyberattacks (Kanwal et al., 2024). Building resilience requires not only technical measures but also organizational preparedness, including clear communication channels, incident response plans, and routine drills.

3. CHALLENGES

There are a lot of challenges as shown in Table-2 in the maritime domain relating to cybersecurity. These are explained in detail below.

Table-2 : Challenges

No	Challenges
1	Lack of Standardization
2	Human Factors
3	Emerging Technologies
4	Geopolitical Tensions
5	Privacy Concerns

3.1. Lack of Standardization

The absence of universally adopted cybersecurity standards creates inconsistencies in how maritime organizations address threats (Kampourakis et al., 2023). This fragmentation complicates efforts to establish a cohesive defense strategy. For example, while some countries adhere to IMO guidelines, others lack the resources or political will to implement them. This inconsistency leaves gaps in cybersecurity defenses, making it easier for attackers to manipulate vulnerabilities across jurisdictions.

Additionally, the lack of standardization extends to technical protocols and communication systems (Adil et al., 2024). Many maritime organizations use proprietary systems that are incompatible with each other, creating silos of information and hindering collaborative defense efforts. For instance, a cyberattack on one organization may not be detected or mitigated effectively if neighboring entities lack the tools or protocols to distribute threat intelligence.

3.2. Human Factors

Human error remains a significant vulnerability (Popli et al., 2025). Insufficient training and awareness among maritime personnel often lead to inadvertent breaches, such as phishing attacks or misconfigured systems. According to a 2022 report by Verizon, 85% of successful cyberattacks involve human error.

Addressing this issue needs comprehensive training programs and a culture of cybersecurity awareness.

Crew members and shore-based staff often lack the technical expertise to identify and respond to sophisticated cyber threats (Eren et al., 2024). For example, phishing emails disguised as legitimate communications from port authorities or shipping agents can trick employees into divulging sensitive information. Additionally, poor password hygiene and failure to update software regularly worsen vulnerabilities.

To mitigate these risks, organizations must invest in tailored training programs that simulate real-world cyberattack scenarios (Božić, 2023). For instance, tabletop exercises can help staff practice responding to incidents such as ransomware attacks or data breaches. Regular drills and workshops can reinforce best practices, such as recognizing phishing attempts and securing private devices.

3.3. Emerging Technologies

While technologies like IoT and AI offer transformative benefits, they also introduce new risks (Demirezen and Selcen Navruz, 2023). For instance, interconnected systems increase the attack surface, making it easier for cybercriminals to infiltrate networks. Autonomous ships, while reducing labor costs, rely heavily on software that can be hacked, potentially generating catastrophic accidents or unauthorized access to sensitive data.

IoT devices, which are widely used for monitoring cargo conditions, engine performance, and navigation systems, often lack robust security features (Gençoğlu, 2022). Many IoT devices are shipped with default passwords that users rarely change, making them easy targets for attackers. Once compromised, these devices can serve as access points for larger-scale attacks on maritime networks.

Similarly, AI-powered systems, while enhancing efficiency, can be manipulated by adversaries (Damar et al., 2024). For example, attackers could feed false data into AI algorithms used for route optimization, causing vessels to take inefficient or dangerous paths. Autonomous ships, which rely entirely on software for navigation and decision-making, are particularly vulnerable to opposing attacks that exploit weaknesses in machine learning models.

3.4. Geopolitical Tensions

The maritime domain is often a battleground for geopolitical conflicts, with state-sponsored cyberattacks targeting critical infrastructure (Altunay, 2024). Such attacks not only disrupt operations but also compromise sensitive data. For example, the 2021 SolarWinds hack highlighted the susceptibility of supply chains to sophisticated cyber espionage.

State-sponsored actors may target maritime infrastructure to achieve strategic objectives, such as disrupting trade routes or gaining access to classified military information (Afenyo and Caesar, 2023). For instance, cyberattacks on ports controlled by rival nations can cripple economic activity and create diplomatic tensions. In some cases, attackers may aim to plunder intellectual property related to ship design, navigation systems, or logistics management.

The global nature of the maritime industry complicates efforts to attribute cyberattacks to specific actors (Yoşumaz, 2024). Attackers often use proxies or obfuscation techniques to mask their identities, making it difficult for victims to pursue legal action or retaliate. This ambiguity undermines trust between nations and burdens international cooperation on cybersecurity.

3.5. Privacy Concerns

The collection and storage of vast amounts of data from sensors, communication systems, and crew/passenger records raise privacy issues (Avcı, 2023). Ensuring compliance with regulations while maintaining operational efficiency is a delicate balance. For instance, tracking systems used for navigation and safety can recklessly expose individuals' locations.

Maritime organizations collect sensitive data about crew members, passengers, and cargo (Eren et al., 2024). This includes biometric information, travel histories, and financial details. If improperly secured, this data can be exploited for identity theft, fraud, or espionage. For example, a breach of passenger records could disclose sensitive information about high-profile individuals traveling aboard luxury cruise liners.

Regulatory frameworks such as GDPR impose strict requirements on how organizations handle personal data. However, compliance can be challenging for maritime companies operating across multiple jurisdictions. Differences in privacy laws between countries create confusion and increase the risk of non-compliance (Jo et al., 2022). Moreover, the sheer volume of data generated by

modern maritime systems makes it difficult to actualize effective data protection measures.

4. FUTURE PROSPECTS

There are four future prospects as shown in Figure-1 in the maritime domain relating to cybersecurity.

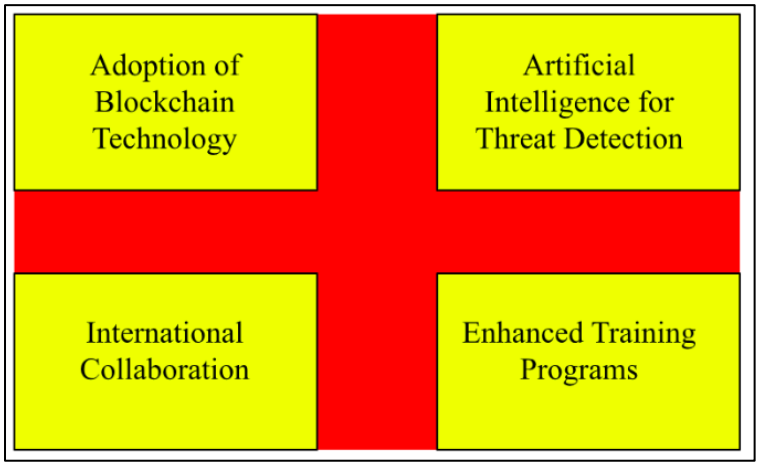

Figure-1 : Future Prospects

4.1. Adoption of Blockchain Technology

Blockchain offers a decentralized and tamper-proof solution for securing maritime transactions and data exchanges (Avcı, 2023). Its application could enhance transparency and trust in supply chain operations. For example, blockchain-based smart contracts can automate payments and decrease fraud.

One promising use case for blockchain is in verifying the authenticity of cargo documentation (Coşar et al., 2024). By storing bills of lading, certificates of origin, and customs declarations on a blockchain, stakeholders can ensure that documents have not been altered or forged. This reduces the risk of disputes and streamlines the customs clearance method.

Blockchain can also enhance cybersecurity by providing immutable logs of system activity (Topal and Altan, 2024). For instance, recording all access attempts and configuration changes on a blockchain ensures that any unauthorized actions can be traced back to their source. This capability is

particularly valuable for detecting insider threats or unauthorized qualifications to critical systems.

However, implementing blockchain solutions requires overcoming several challenges. These include ensuring interoperability with legacy systems, addressing scalability issues, and educating stakeholders about the advantages and limitations of blockchain technology.

4.2. Artificial Intelligence for Threat Detection

AI-driven tools can analyze vast datasets to identify anomalies and predict potential threats (Kanwal et al., 2024). Machine learning algorithms can adapt to evolving attack patterns, providing real-time protection. For instance, AI-powered intrusion detection systems can observe network traffic and flag suspicious activities.

AI can also enhance situational awareness by correlating data from multiple sources, such as radar, AIS (Automatic Identification System), and weather forecasts (Altunay, 2024). For example, AI algorithms can detect unusual vessel movements that may indicate smuggling, piracy, or illegal fishing activities. This efficiency enables authorities to respond more quickly and effectively to security threats.

Despite its potential, AI also introduces new risks. Adversaries can exploit weaknesses in AI models to launch adversarial attacks, where small perturbations in input data cause incorrect predictions (Avcı, 2023). For instance, attackers could manipulate sensor readings to mislead AI systems responsible for collision avoidance or route planning. To relieve these risks, organizations must adopt robust testing and validation procedures when deploying AI solutions.

4.3. International Collaboration

Strengthening international cooperation through treaties and information-sharing agreements will be crucial for combating cross-border cyber threats. Initiatives like the IMO's Facilitation Committee are steps in the right direction (Chaal et al., 2023). Collaborative efforts can also help reconcile standards and share best practices.

International collaboration is essential for addressing the global nature of maritime cybersecurity threats (Jo et al., 2022). For example, joint exercises involving multiple countries can test the effectiveness of incident response plans

and improve coordination during crises. Sharing threat intelligence through platforms like the Maritime Information Sharing and Analysis Center (M-ISAC) enables organizations to stay informed about arising threats and vulnerabilities.

Governments can also play a role by establishing regulatory frameworks that incentivize cybersecurity investments (Coşar et al., 2024). For instance, tax breaks or subsidies could encourage smaller operators to adopt advanced security measures. Additionally, public-private partnerships can ease knowledge transfer and resource sharing between governments and industry players.

4.4. Enhanced Training Programs

Investing in cybersecurity education and training for maritime personnel will reduce human-related vulnerabilities (Bolbot et al., 2023). Simulated exercises and workshops can prepare staff for real-world scenarios. For example, tabletop exercises can pretend to be cyberattack scenarios and test response plans.

Training programs should cover a wide range of topics, including basic cybersecurity hygiene, incident response procedures, and the use of specialized tools (Afenyo and Caesar, 2023). For instance, crew members should learn how to recognize phishing emails, avoid downloading unverified software, and report suspicious activities promptly. Shore-based staff, such as IT administrators and logistics managers, require more advanced training on securing networks, managing access controls, and conducting juridical investigations.

To maximize the impact of training programs, organizations should adopt a continuous learning approach (Popli et al., 2025). This involves providing regular updates on emerging threats and offering refresher courses to reinforce key concepts. Gamification techniques, such as simulated hacking competitions, can make training more charming and memorable.

5. CASE STUDIES

There is no single, definitive number for how many cybersecurity attacks have been made against the maritime domain globally, as many incidents go unreported, are under-investigated, or are not publicly disclosed due to commercial or security concerns. However, cybersecurity threats to the maritime sector have been increasing significantly in recent years as shown in Figure-2 due to the growing digitalization of shipping operations, port management systems, navigation technologies, and supply chain logistics. These incidents have been

reported to BIMCO and IMO, and this figure has been formed with the help of Maritime Cyber Attack Database (MCAD) NHL Stenden University

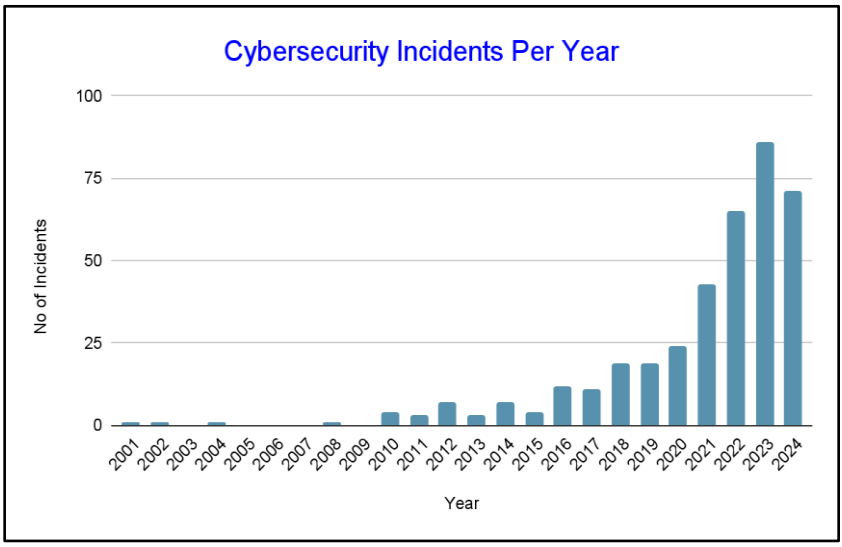

Figure-2 : Cyber Incidents in Maritime Domain

To better understand the real-world implications of cybersecurity and privacy challenges in the maritime domain, this section presents several case studies that highlight notable cyber incidents and their impacts. The case studies are shown in Table 3-14 below.

These events have deeply influenced and affected the maritime domain for good and bad. Several resources, goods, workforce, security approaches, and stakeholders have been under pressure. The case studies have been researched and with the help of this impact and learned lessons have been put forth. These events related to cybersecurity in the maritime domain have been cornerstones according to IMO, UN, and NATO. These organizations have developed some measures to ensure safety and security at sea.

Table-3 : Case Study 1: The NotPetya Ransomware Attack on Maersk (2017)

Background	Impact	Lessons Learned
In June 2017, the global shipping giant A.P. Moller-Maersk fell victim to the NotPetya ransomware attack,	**Operational Disruptions:** Maersk's IT systems were crippled, leading to delays in cargo handling and shipping schedules. Ports operated by Maersk, such as those in	The NotPetya attack underscored the importance of robust backup systems and disaster recovery plans. It

which originated as a cyberweapon targeting Ukrainian businesses but quickly spread worldwide. The attack encrypted critical data and disrupted operations across Maersk's global network, including its container terminals, logistics platforms, and customer-facing systems.	Rotterdam and Los Angeles, experienced significant backlogs.	also demonstrated how interconnected systems can amplify the impact of a single breach, affecting multiple stakeholders across the supply chain.
	Financial Losses: The company reported losses exceeding $300 million due to the attack. Recovery efforts required rebuilding thousands of servers and reinstalling software across its infrastructure.	
	Reputational Damage: The incident highlighted vulnerabilities in the maritime sector and raised concerns among customers about the reliability of digital systems.	

Table-4 : Case Study 2: GPS Spoofing Incidents in the Black Sea (2017)

Background	Impact	Lessons Learned
In June 2017, multiple vessels operating in the Black Sea reported anomalies with their GPS systems. Ships' navigation systems displayed incorrect positions, placing them miles away from their actual locations. Investigations suggested that the incidents were caused by GPS spoofing—a technique where attackers broadcast false signals to mislead receivers.	**Navigation Errors:** Misleading GPS data could lead to collisions, groundings, or unauthorized entry into restricted zones.	The Black Sea incidents emphasize the need for resilient navigation systems that can detect and mitigate spoofing attempts. Technologies like multi-sensor fusion, which combines GPS data with inertial navigation and radar inputs, can reduce reliance on vulnerable satellite signals.
	Economic Consequences: Delays and rerouting resulting from spoofed coordinates increased operational costs for shipping companies.	
	Geopolitical Implications: The attacks were attributed to state-sponsored actors seeking to assert dominance in contested waters, highlighting the intersection of cybersecurity and geopolitics.	

Table-5 : Case Study 3: The COSCO Shipping Cyberattack (2018)

Background	Impact	Lessons Learned
In July 2018, COSCO Shipping, one of the world's largest shipping companies, suffered a cyberattack that disrupted its operations in the Americas. The attack targeted the company's network infrastructure, causing widespread outages in email, phone, and data processing systems.	**Communication Breakdown:** The outage affected communication between COSCO offices and customers, leading to delays in cargo bookings and shipments.	The incident demonstrated the cascading effects of cyberattacks on interconnected supply chains. It also underscored the importance of redundant communication systems and transparent crisis management strategies.
	Reputational Damage: Customers expressed frustration over the lack of transparency during the recovery process, which damaged COSCO's reputation as a reliable logistics provider.	
	Global Ripple Effects: The disruption impacted global supply chains, particularly for industries reliant on just-in-time delivery.	

Table-6 : Case Study 4: The Stuxnet-Like Attack on Iranian Oil Tankers (2019)

Background	Impact	Lessons Learned
In 2019, Iranian oil tankers reportedly fell victim to a sophisticated cyberattack resembling the infamous Stuxnet malware. The attack targeted industrial control systems (ICS) used to manage tanker operations, including navigation and engine controls.	**System Malfunctions:** The malware caused erratic behavior in onboard systems, including sudden changes in speed and course deviations, posing safety risks to crew members and nearby vessels.	This case study illustrates the dangers of targeting operational technology (OT) in maritime environments. It highlights the need for enhanced security measures for ICS and greater international cooperation to address state-sponsored cyber threats.
	Geopolitical Tensions: The attack was attributed to state-sponsored actors, exacerbating tensions in the region and highlighting the use of cyberweapons in maritime conflicts.	

	Environmental Risks: Compromised tanker systems raised concerns about potential oil spills or environmental disasters.	

Table-7 : Case Study 5: The Port of Barcelona Cyberattack (2020)

Background	Impact	Lessons Learned
In December 2020, the Port of Barcelona suffered a cyberattack that targeted its administrative systems. Hackers gained access to sensitive data, including employee records and financial information, through a phishing email campaign.	**Data Breach:** Personal data of employees and contractors was compromised, raising privacy concerns and potential legal liabilities under GDPR.	The incident highlights the importance of securing both operational technology (OT) and information technology (IT) systems. It also underscores the need for comprehensive training programs to prevent phishing attacks and other human errors.
	Operational Delays: While core port operations remained unaffected, administrative functions were disrupted, delaying customs clearances and other processes.	
	Trust Erosion: The breach damaged the port's reputation, prompting calls for stricter cybersecurity measures.	

Table-8 : Case Study 6: The Hack of Mediterranean Cruise Line Passenger Data (2020)

Background	Impact	Lessons Learned
In early 2020, a major Mediterranean cruise line suffered a data breach that exposed the personal information of thousands of passengers. Attackers gained unauthorized access to the company's reservation system through a third-party vendor with weak security controls.	**Privacy Violations:** Sensitive passenger data, including passport details, credit card numbers, and travel itineraries, was leaked online, violating GDPR requirements.	This case highlights the risks associated with third-party vendors and the importance of vetting suppliers' cybersecurity practices. It also underscores the need for encryption and access controls to protect sensitive customer data.
	Customer Trust Erosion: Passengers filed complaints and lawsuits, accusing the company of negligence in protecting their data.	
	Regulatory Penalties: The cruise line faced hefty fines from European regulators for failing to implement adequate safeguards.	

Table-9 : Case Study 7: The Colonial Pipeline Ransomware Attack (2021)

Background	Impact	Lessons Learned
Although not directly related to maritime operations, the Colonial Pipeline ransomware attack serves as a cautionary tale for the broader energy and transportation sectors. In May 2021, the DarkSide ransomware group infiltrated Colonial Pipeline's IT systems, forcing the company to shut down its fuel distribution network temporarily.	**Supply Chain Disruptions:** The shutdown led to widespread fuel shortages along the U.S. East Coast, causing panic buying and price spikes. **Ransom Payment:** Colonial Pipeline paid a $4.4 million ransom in Bitcoin to restore operations, though only a portion was later recovered by law enforcement. **Regulatory Scrutiny:** The incident prompted increased scrutiny of critical infrastructure cybersecurity and led to new mandates for pipeline operators to implement stronger defenses.	Ports and offshore energy platforms face similar risks, as they rely on interconnected systems for logistics and production. A cyberattack on a port's fuel storage facility or an offshore rig could have equally devastating consequences, disrupting energy supplies and causing environmental damage.

Table-10 : Case Study 8 : The Panama Canal Cybersecurity Incident (2021)

Background	Impact	Lessons Learned
In late 2021, the Panama Canal Authority detected a cyber intrusion targeting its scheduling and billing systems. While no physical damage occurred, the attackers attempted to disrupt traffic flow by altering vessel transit schedules.	**Operational Delays:** Temporary disruptions in scheduling caused minor delays for vessels awaiting passage through the canal. **Economic Losses:** Shipping companies faced additional costs due to rescheduling and rerouting. **Heightened Security Measures:** The incident prompted the authority to invest in advanced threat detection systems and employee training programs.	The incident reinforced the importance of securing critical infrastructure against both direct and indirect cyber threats. It also highlighted the role of human vigilance in detecting and mitigating suspicious activities.

Table-11 : Case Study 9: The Port of Long Beach Ransomware Attack (2021)

Background	Impact	Lessons Learned
In September 2021, the Port of Long Beach, one of the busiest ports in the United States, experienced a ransomware attack that targeted its administrative and logistics systems. The attackers exploited vulnerabilities in outdated software and unpatched systems to gain access to sensitive data, including shipping manifests, employee records, and financial transactions.	**Operational Disruptions:** While the port's core operations were not directly affected, delays in customs clearance and cargo handling caused significant backlogs. Shipping companies faced increased costs due to extended wait times. **Data Breach:** Personal information of employees and contractors was compromised, raising concerns about privacy violations under GDPR and CCPA regulations. **Financial Costs:** The port incurred substantial expenses for incident response, forensic investigations, and system upgrades to prevent future attacks.	The attack highlighted the importance of maintaining up-to-date software and implementing robust patch management practices. It also emphasized the need for segmentation between IT and OT systems to limit the spread of malware.

Table-12 : Case Study 10: Blockchain Implementation in the Port of Antwerp (2022)

Background	Impact	Lessons Learned
The Port of Antwerp implemented blockchain technology to enhance transparency and security in its supply chain operations. The initiative involved creating a decentralized ledger to track cargo movements, verify documentation, and automate payments using smart contracts.	**Improved Efficiency:** Automated processes reduced paperwork and streamlined customs clearance, saving time and resources. **Enhanced Security:** Immutable records ensured that documents could not be altered or forged, reducing the risk of fraud. **Industry Leadership:** The project set a benchmark for other ports considering blockchain adoption, demonstrating its potential to transform maritime logistics.	Blockchain offers promising solutions for enhancing cybersecurity and privacy in the maritime domain. However, successful implementation requires overcoming technical challenges, such as scalability and interoperability, and ensuring stakeholder buy-in.

Table-13 : Case Study 11: The Singapore Maritime Cybersecurity Exercise (2022)

Background	Impact	Lessons Learned
In 2022, Singapore conducted a large-scale cybersecurity exercise involving multiple government agencies, port operators, and private sector stakeholders. The exercise simulated a coordinated cyberattack on critical maritime infrastructure, including ports, vessels, and offshore installations.	**Improved Coordination:** Participants identified gaps in communication and response protocols, leading to the development of more effective incident response plans. **Public Awareness:** The exercise raised awareness among industry players about the importance of cybersecurity preparedness. **Policy Changes:** Insights from the exercise informed updates to Singapore's maritime cybersecurity regulations, emphasizing mandatory risk assessments and regular drills.	The exercise demonstrated the value of proactive testing and collaboration in strengthening maritime cybersecurity. It also showed how simulations can help organizations identify vulnerabilities before real-world incidents occur.

Table-14 : Case Study 12: The Autonomous Ship Trial Hacking Incident (2023)

Background	Impact	Lessons Learned
During a trial run of an autonomous ship in Norway in 2023, researchers discovered vulnerabilities in the vessel's AI-based navigation system. By feeding false data into the system, they were able to manipulate the ship's route, causing it to deviate significantly from its intended path.	**Safety Risks:** The manipulated routes posed collision risks and could have led to grounding or other accidents. **Trust Issues:** The incident raised doubts about the reliability of autonomous ships and slowed regulatory approval processes. **Technological Gaps:** It revealed weaknesses in AI models and the lack of robust anomaly detection mechanisms.	The trial exposed the challenges of securing AI-powered systems against adversarial attacks. It emphasized the need for rigorous testing and validation of autonomous technologies before deployment.

6. RESULTS AND DISCUSSION

6.1. Key Findings from the Analysis

Our analysis exposes several critical insights into the state of cybersecurity and privacy in the maritime domain as shown in Figure-3. These findings are categorized into four main areas as fragmentation, emerging threats, human factors, and opportunities for innovation.

6.1.1 Fragmentation in Cybersecurity Practices

One of the most important challenges identified is the lack of standardization across the maritime industry. While frameworks like the IMO Guidelines and NIST Cybersecurity Framework provide foundational guidance, their adoption varies widely between organizations and jurisdictions. For example, large shipping companies may have the resources to implement advanced cybersecurity measures, while smaller operators often struggle to meet even basic requirements. This disparity creates gaps in defenses, leaving the entire ecosystem sensitive to cascading attacks.

Additionally, the absence of universal technical standards complicates interoperability. Many maritime systems rely on proprietary protocols that are incompatible with others, hindering information sharing and collaborative defense efforts. For instance, a cyberattack on one port's cargo management system could go undetected by neighboring ports if they lack the devices or protocols to share threat intelligence.

6.1.2 Emerging Threats Outpacing Defenses

The rapid pace of technological innovation in the maritime sector has outstripped the ability of regulatory bodies and organizations to keep up. For example, the proliferation of IoT devices has introduced new attack vectors, yet many devices remain unsecured due to outdated firmware or default passwords. Similarly, AI-powered systems designed to optimize operations can be manipulated by adversaries through adversarial attacks, where small changes in input data lead to wrong outputs.

Another emerging threat is the rise of state-sponsored cyberattacks targeting critical maritime infrastructure. These attacks often involve sophisticated techniques, such as supply chain compromises or zero-day exploits, making them

difficult to detect and mitigate. The SolarWinds hack of 2021 serves as a stark reminder of how deeply embedded vulnerabilities can be exploited to infiltrate even the most protected networks.

6.1.3 Human Factors as a Persistent Weakness

Despite advances in technology, humans remain the weakest link in the cybersecurity chain. Insufficient training and awareness among maritime personnel often lead to inadvertent breaches, such as phishing attacks or misconfigured systems. According to Verizon's 2022 Data Breach Investigations Report, 85% of successful cyberattacks involve human error. In the maritime context, crew members and shore-based staff frequently lack the technical expertise to determine and respond to sophisticated threats.

For example, phishing emails disguised as legitimate communications from port authorities or shipping agents can trick employees into divulging sensitive information. Poor password hygiene and failure to update software regularly further exacerbate vulnerabilities. Addressing these issues needs not only technical solutions but also a cultural shift toward greater cybersecurity awareness.

6.1.4 Opportunities for Innovation

Technologies like blockchain and AI offer promising solutions to enhance cybersecurity and privacy in the maritime domain. Blockchain, for instance, can provide immutable logs of system activity, ensuring transparency and accountability. It can also streamline supply chain operations by validating the authenticity of cargo documentation and automating payments through smart contracts.

AI-driven tools, on the other hand, can analyze vast datasets to identify anomalies and predict potential threats. Machine learning algorithms can adapt to evolving attack patterns, providing real-time protection. For example, AI-powered intrusion detection systems can monitor network traffic and flag doubtful activities before an attack occurs.

However, implementing these technologies requires careful consideration of their limitations. Blockchain solutions must address scalability issues and ensure interoperability with legacy systems, while AI models must be rigorously tested to hinder adversarial attacks.

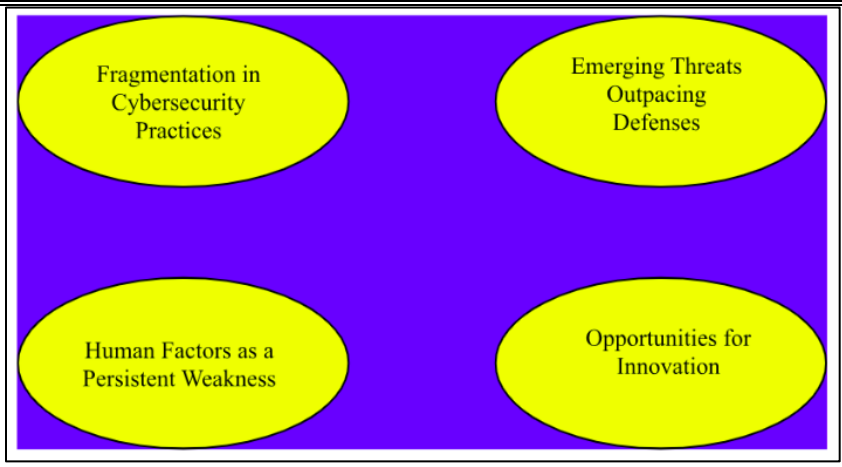

Figure-3 : Key Findings from the Analysis

6.2. Implications for Stakeholders

The findings from our analysis have crucial implications for various stakeholders in the maritime domain as shown in Figure-4.

6.2.1. Shipping Companies

Must prioritize investments in cybersecurity infrastructure, including firewalls, intrusion detection systems, and employee training programs. They should also adopt risk-based approaches to assess vulnerabilities and allocate resources efficiently.

6.2.2. Port Authorities

Need to enhance coordination with neighboring ports and government agencies to share threat intelligence and develop unified response plans. Implementing standardized protocols for communication and data exchange will enhance collective defenses.

6.2.3. Regulatory Bodies

Should work toward harmonizing cybersecurity standards across jurisdictions to reduce fragmentation. This includes updating regulations to reflect the complexities of modern maritime operations and motivating compliance through tax breaks or subsidies.

6.2.4. Technology Providers

Play a crucial role in developing secure and scalable solutions tailored to the unique needs of the maritime industry. Collaborating with end-users during the design phase can help ensure that products meet both functional and security requirements.

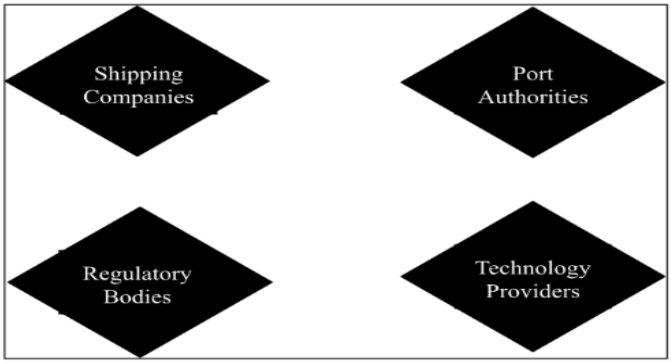

Figure-4 : Implications for Stakeholders

CONCLUSION

Cybersecurity and privacy in the maritime domain are complex and multifaceted challenges that require urgent attention. As the industry continues to embrace digital transformation, stakeholders must adopt a proactive and holistic approach to safeguard operations against growing threats. A new model as shown in Figure-5 as main results of the research have been put forth.

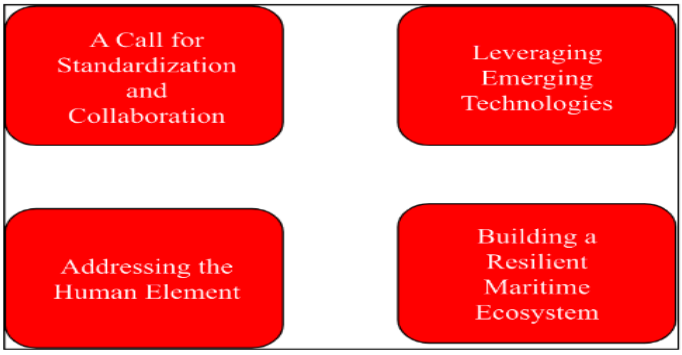

Figure-5 : Main Results

1. A Call for Standardization and Collaboration

One of the most pressing priorities is the establishment of universally adopted cybersecurity standards. Without standardized frameworks, organizations operate in silos, creating inconsistencies in how threats are addressed. Harmonizing practices across jurisdictions will enable better information sharing and foster trust among stakeholders. Initiatives like the IMO's Facilitation Committee represent important steps in this direction, but more work is needed to achieve extensive adoption.

International collaboration is equally vital. Given the global nature of the maritime industry, no single organization or country can tackle cybersecurity challenges alone. Joint exercises involving multiple nations can test the effectiveness of incident response plans and improve coordination during crises. Platforms like the Maritime Information Sharing and Analysis Center (M-ISAC) facilitate the exchange of threat intelligence, enabling organizations to stay informed about rising risks.

2. Leveraging Emerging Technologies

Emerging technologies such as blockchain and AI hold immense potential to transform maritime cybersecurity. Blockchain can enhance transparency and trust by providing tamper-proof records of transactions and system activity. For example, storing bills of lading and customs declarations on a blockchain ensures that documents cannot be changed or forged, reducing the risk of fraud and disputes.

AI, meanwhile, can revolutionize threat detection and response capabilities. By analyzing vast amounts of data in real time, AI-powered tools can identify anomalies and predict potential attacks before they occur. For instance, machine learning algorithms can detect unusual vessel movements that may indicate smuggling or piracy activities, enabling authorities to respond more promptly and effectively.

However, leveraging these technologies requires overcoming several challenges. Blockchain solutions must address scalability issues and ensure compatibility with existing systems, while AI models must be rigorously tested to prevent adversarial attacks. Organizations must also invest in robust testing

and validation processes to ensure that new technologies do not introduce further vulnerabilities.

3. Addressing the Human Element

While technology plays a critical role in enhancing cybersecurity, addressing human factors remains equally important. Comprehensive training programs that simulate real-world cyberattack scenarios can prepare staff to respond effectively to incidents. Regular drills and workshops reinforce best practices, such as recognizing phishing attempts and safeguarding personal devices.

To maximize the impact of training programs, organizations should adopt a continuous learning approach. Providing regular updates on emerging threats and offering refresher courses helps reinforce key concepts. Gamification techniques, such as simulated hacking competitions, make training more engaging and noteworthy.

4. Building a Resilient Maritime Ecosystem

Ultimately, the goal is to build a resilient maritime ecosystem that can withstand and recover from cyberattacks. This requires a multi-layered approach that integrates technical, regulatory, and human-centric strategies. Organizations must continuously assess vulnerabilities, prioritize mitigation efforts, and invest in forefront technologies.

Governments, industry players, and cybersecurity experts must collaborate to develop unified strategies that address the unique challenges of the maritime environment. By doing so, they can create a safer, more secure maritime ecosystem that supports global trade and welfare.

In conclusion, the future of maritime cybersecurity depends on the collective efforts of all stakeholders. By adopting a proactive and holistic approach, the maritime industry can navigate the complexities of digital transformation and ensure safe, secure, and private operations in a progressively interconnected world.

As a new model; A Call for Standardization and Collaboration, Leveraging Emerging Technologies, Addressing the Human Element, and Building a Resilient Maritime Ecosystem should be implemented in all maritime domains.

REFERENCES

Adil, M., Khan, M. K., Kumar, N., Attique, M., Farouk, A., Guizani, M., and Jin, Z. P. (2024). Healthcare internet of things: security threats, challenges, and future research directions. *IEEE Internet of Things Journal*, *11*(11), 19046–19069. https://doi.org/10.1109/JIOT.2024.3360289

Afenyo, M., and Caesar, L. D. (2023). Maritime cybersecurity threats: gaps and directions for future research. *Ocean & Coastal Management*, *236*. https://doi.org/10.1016/j.ocecoaman.2023.106493

Akdag, M., Solnor, P., and Johansen, T. A. (2022). Collaborative collision avoidance for maritime autonomous surface ships: a review. *Ocean Engineering*, *250*. https://doi.org/10.1016/j.oceaneng.2022.110920

Altunay, H. C. (2024). Analysis of cyber attacks using honeypot. *Black Sea Journal of Engineering and Science*, *7*(5), 954–959. https://doi.org/10.34248/bsengineering.1531420

Avcı, İ. (2023). Cyber-attacks and measures in smart transportation systems. *Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi*, *6*(1), 194–208. https://doi.org/10.51513/jitsa.1224909

Berghout, T., Benbouzid, M., and Muyeen, S. M. (2022). Machine learning for cybersecurity in smart grids: a comprehensive review-based study on methods, solutions, and prospects. *International Journal of Critical Infrastructure Protection*, *38*. https://doi.org/10.1016/j.ijcip.2022.100547

Bolbot, V., Van Coillie, A. (2023). A novel risk assessment process: application to an autonomous inland waterways ship. *Proceedings of The Institution of Mechanical Engineers Part O-Journal of Risk and Reliability*, *237*(2), 436–458. https://doi.org/10.1177/1748006X211051829

Božić, V. (2023). Integrated risk management and artificial intelligence in hospital. *Journal of AI*, *7*(1), 63–80. https://doi.org/10.61969/jai.1329224

Chaal, M., Ren, X., BahooToroody, A., Basnet, S., Bolbot, V., Banda, O. A. V, and Van Gelder, P. (2023). Research on risk, safety, and reliability of autonomous ships: a bibliometric review. *Safety Science*, *167*. https://doi.org/10.1016/j.ssci.2023.106256

Coşar, H. İ., Arısoy, Ç., and Ulutaş, H. (2024). Intrusion detection on CSE-CIC-IDS2018 dataset using machine learning methods. *Artificial Intelligence*

Theory and Applications, *4*(2), 143–154. https://dergipark.org.tr/tr/pub/aita/issue/87553/1553769

Damar, M., Özen, A., and Yılmaz, A. (2024). Cybersecurity in the health sector in the reality of artificial intelligence, and information security conceptually. *Journal of AI*, *8*(1), 61–82. https://doi.org/10.61969/jai.1466340

Demirezen, M. U., and Selcen Navruz, T. (2023). Lambda architecture-based big data system for large-scale targeted social engineering email detection. *International Journal of Information Security Science*, *12*(3), 29–59. https://doi.org/10.55859/ijiss.1338813

Durlik, I., Miller, T., Kostecka, E., Zwierzewicz, Z., and Lobodzinska, A. (2024). Cybersecurity in autonomous vehicles-are we ready for the challenge? *Electronics*, *13*(13). https://doi.org/10.3390/electronics13132654

Eren, T., Sanlı, Y. B., Baltacı, F., and Güven, E. (2024). Bibliometric analysis on cybersecurity studies. *Bilişim Teknolojileri Dergisi*, *17*(3), 223–229. https://doi.org/10.17671/gazibtd.1473206

Gençoğlu, M. T. (2022). Mathematical modeling of cyber attack and defense. *Bilgisayar Bilimleri ve Teknolojileri Dergisi*, *3*(1), 10–16. https://doi.org/10.54047/bibted.997908

Jo, Y., Choi, O., You, J., Cha, Y., and Lee, D. H. (2022). Cyberattack models for ship equipment based on the MITRE attack framework. *Sensors*, *22*(5). https://doi.org/10.3390/s22051860

Jovic, M., Tijan, E., Brcic, D., and Pucihar, A. (2022). Digitalization in maritime transport and seaports: bibliometric, content and thematic analysis. *Journal of Marine Science and Engineering*, *10*(4). https://doi.org/10.3390/jmse10040486

Kampourakis, V., Gkioulos, V., and Katsikas, S. (2023). A systematic literature review on wireless security test beds in the cyber-physical realm. *Computers & Security*, *133*. https://doi.org/10.1016/j.cose.2023.103383

Kanwal, K., Shi, W. M., Kontovas, C., Yang, Z. L., and Chang, C. H. (2024). Maritime cybersecurity: are onboard systems ready?, *Maritime Policy & Management*, *51*(3), 484–502. https://doi.org/10.1080/03088839.2022.2124464

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., and Apostolou, P. (2022). Digital transformation of the maritime industry: a cybersecurity systemic

approach. *International Journal of Critical Infrastructure Protection, 37*. https://doi.org/10.1016/j.ijcip.2022.100526

Khandker, S., Turtiainen, H., Costin, A., and Hämäläinen, T. (2022). Cybersecurity attacks on software logic and error handling within ais implementations: a systematic testing of resilience. *IEEE Access, 10*, 29493–29505. https://doi.org/10.1109/ACCESS.2022.3158943

Park, C., Kontovas, C., Yang, Z. L., and Chang, C. H. (2023). A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean & Coastal Management, 235*. https://doi.org/10.1016/j.ocecoaman.2023.106480

Popli, M. S., Singh, R. P., Popli, N. K., and Mamun, M. (2025). A federated learning framework for enhanced data security and cyber intrusion detection in distributed network of underwater drones. *IEEE Access, 13*, 12634–12646. https://doi.org/10.1109/ACCESS.2025.3530499

Qiao, M. Y., Wei, L. F., Han, D. Z., and Wu, H. F. (2025). Efficient multi-party PSI and its application in port management. *Computer Standards & Interfaces, 91*. https://doi.org/10.1016/j.csi.2024.103884

Tedeschi, P., Sciancalepore, S., and Di Pietro, R. (2022). Satellite-based communications security: A survey of threats, solutions, and research challenges. *Computer Networks, 216*. https://doi.org/10.1016/j.comnet.2022.109246

Topal, M., and Altan, Z. (2024). Impact of digital signing on malware in public key infrastructure. *International Journal of Management Information Systems and Computer Science, 8*(2), 99–109. https://doi.org/10.33461/uybisbbd.1507316

Wang, W. (2024). Innovative strategies and forward thinking on China's digital maritime law enforcement. *Marine Policy, 169*. https://doi.org/10.1016/j.marpol.2024.106369

Yoşumaz, İ. (2024). An examination of cyber security solutions in public and private IaaS infrastructures. *International Journal of Information Security Science, 13*(3), 1–29. https://doi.org/10.55859/ijiss.1475423