Research Article
Turkish Journal of Maritime and Marine Sciences

DOI: 10.52998/trjmms.1531187
Volume: 10 Special Issue: 1 (2024) 51-61

A Comprehensive Analysis of Maritime Cyber Security Incidents: Trends, Impacts, and Countermeasures

Denizcilik Sektöründe Siber Güvenlik Olaylarının Kapsamlı Analizi: Trendler, Etkiler ve Karşı Önlemler

Türk Denizcilik ve Deniz Bilimleri Dergisi

Cilt: 10 Özel Sayı: 1 (2024) 51-61

Emre DÜZENLİ[1], Gizem KAYİŞOĞLU[1,*] Tayfun ACARER[2], Pelin BOLAT[1], Ayşe NAK[1]

[1]*Istanbul Technical University, Maritime Faculty, 3940, Istanbul, Turkiye*
[2]*Piri Reis University, Maritime Faculty, 34940, Istanbul, Turkiye*

ABSTRACT

The maritime industry is currently experiencing a process of digital transformation, which involves a significant level of automation and enhanced communication with external networks. As a result, various facilities in the maritime sector such as commercial and navy vessels, shipping companies, ports, and shipbuilders, are becoming more susceptible to cyber threats. In addition to the potential economic and reputational harm to shipping companies, a cyber-attack on maritime systems could result in significant incidents such as the release of hazardous substances, collisions, grounding, and fires. This poses significant risks to both ship crew, ship, cargo, and environment. This study examines cyber security events in the maritime sector. The main objective is to cultivate a thorough comprehension of cyber-attacks that specifically target systems in maritime facilities, by analyzing insights derived from incidents in the Maritime Cyber-Attack Database. The work involves the construction and examination of a number of cyber security incidents. An inquiry is carried out to determine the time patterns, geographical spread, sector-specific consequences, and attributes of these cyber-attacks, including the identity of the perpetrator, intention (whether deliberate or unintentional), and the affected systems inside the maritime domain. The paper examines particular instances to identify the main stages of a cyber-attack on maritime facilities' systems, the fundamental strategies employed by attackers, and proposes standard cyber security solutions to reduce these risks. The study's contribution entails the methodical delineation of the cyber security terrain that is unique to the maritime industry.

Keywords: Maritime cyber security incident, Maritime cyber security, Cyber incident analysis

Article Info
Received: 10 August 2024
Revised: 05 September 2024
Accepted: 08 September 2024

*(corresponding author)
E-mail: yukselg@itu.edu.tr

To cite this article: Düzenli, E., Kayisoglu, G., Acarer, T., Bolat, P., Nak, A. (2024). A Comprehensive Analysis of Maritime Cyber Security Incidents: Trends, Impacts, and Countermeasures, *Turkish Journal of Maritime and Marine Sciences*, 10 (Special Issue: 1): 51-61. doi: 10.52998/trjmms.1531187.

ÖZET

Denizcilik endüstrisi, kapsamlı otomasyon ve harici ağlarla artan bağlantı ile karakterize edilen dijital bir dönüşümden geçmektedir. Bu durum, deniz tesislerini siber tehditlere karşı savunmasız hale getirmektedir. Nakliye şirketleri için potansiyel ekonomik ve itibar zararının ötesinde, deniz sistemlerine yönelik bir siber saldırı, tehlikeli maddelerin boşaltılması, çarpışmalar, karaya oturma, yangınlar gibi ciddi olaylara yol açabilir ve dolayısıyla hem deniz personeli hem de çevre için önemli tehlikeler yaratabilir. Bu çalışma, denizcilik endüstrisindeki siber güvenlik olaylarını araştırmaktadır. Birincil amaç, geçmiş olaylardan içgörüler çıkararak deniz tesislerindeki sistemleri hedef alan siber saldırılar hakkında kapsamlı bir anlayış geliştirmektir. Çalışma, NHL Stenden Uygulamalı Bilimler Üniversitesi'ne ait Deniz Siber Saldırı Veritabanı'ndan (MCAD) toplanan 146 siber güvenlik olayını analiz etmektedir. Saldırganın kimliği, niyet (kasıtlı veya kazara) ve denizcilik alanı kapsamında etkilenen sistemler dahil olmak üzere bu siber saldırıların zamansal kalıplarını, mekansal dağılımını, sektörel etkilerini ve özelliklerini ayırt etmek için bir araştırma yürütülmüştür. Belirli olayları inceleyerek, çalışma deniz tesislerindeki sistemlere yönelik bir siber saldırının temel aşamalarını, saldırganlar tarafından kullanılan birincil taktikleri belirler ve bu tür tehditleri azaltmak için tipik siber güvenlik önlemlerini önerir. Çalışmanın katkısı, denizcilik sektörüne özgü siber güvenlik manzarasının sistematik haritalanmasını sağlar.

Anahtar Kelimeler: Denizel alanda siber güvenlik olayları, Denizel alanda siber güvenlik, Siber güvenlik olay analizi

1. INTRODUCTION

The maritime industry has seen a significant digital revolution in recent years, characterized by the incorporation of enhanced automation and increased communication with external networks (Kyriakides, 2021). The use of digitization has completely transformed the methods used in maritime operations, resulting in significant improvements in productivity and the ability to gather valuable operational knowledge. Nevertheless, amidst these progressions, a significant obstacle arises - the increasing menace of cyber-attacks aimed at maritime facilities (Bolat *et al*., 2016).

As the maritime industry adopts digital technologies to make procedures more efficient and improve communication, it unintentionally becomes vulnerable to a wide range of cyber threats. The merging of operational technology (OT) and information technology (IT) in maritime systems results in a complicated cyber environment, with numerous vulnerabilities and a significant risk of malicious exploitation. Every element within the maritime network, including cargo ships and port infrastructure, can be targeted by cyber attackers with the intention of disrupting operations, causing financial harm, or posing a risk to human life (Farah *et al*., 2022).

The ramifications of a successful cyber-attack on maritime systems go much beyond simply monetary losses or harm to the reputation of shipping corporations (Tam and Jones, 2019). Undoubtedly, these catastrophes have the capacity to trigger disastrous events with significant consequences for both human existence and the environment. Compromised maritime systems can pose serious threats such as the release of hazardous substances, collisions, grounding, and fires (Bernsmed *et al*., 2017). Given these potential dangers, ensuring the cyber security of maritime facilities is of utmost significance, as it not only safeguards assets and infrastructure, but also preserves human safety and environmental integrity.

In light of this context, this study aims to thoroughly investigate cyber security occurrences in the maritime industry. The study aims to gain a detailed understanding of the changing cyber threat landscape in the maritime sector by evaluating a complete dataset of 146 cyber security incidents and extracting insights from prior occurrences. The focus of this effort is to analyze the timing patterns, geographical spread, effects on different sectors, and methods used in cyber-attacks on maritime systems. The study is centered around the Marine Cyber-Attack Database (MCAD), which is a collection of data on cyber security occurrences in the marine industry. The database is managed by NHL Stenden University of Applied Sciences and provides valuable empirical information (NHL STENDEN University of Applied Science, 2001). Using this dataset, the study seeks to uncover the complexities of cyber-attacks on maritime facilities, providing insight into the identities of the attackers, their motives (whether deliberate or unintentional), and the specific systems that are most targeted within the maritime ecosystem.

The study aims to analyze individual occurrences and uncover similarities among different cyber-attacks in order to outline the main stages of an assault on maritime systems, identify the principal strategies used by attackers, and propose effective cyber security measures to reduce these dangers. This study aims to provide stakeholders in the maritime industry with the necessary knowledge and insights to strengthen their ability to withstand cyber-attacks and enhance their defenses against constantly changing cyber threats. The study seeks to provide industry stakeholders, policymakers, and cyber security professionals with practical insights to protect the integrity, security, and sustainability of maritime operations in an increasingly digitalized world by explaining the complex nature of cyber risks faced by maritime facilities.

2. LITERATURE REVIEW

A comprehensive analysis of cyber incidents in the maritime sector reveals a significant number of unreported attacks, emphasizing the need for improved threat information sharing. These incidents, often with low frequency but high impact, are difficult to predict and prepare for, and are carried out by a variety of attackers using different techniques (Meland *et al*., 2021). The maritime industry's cyber security policy, cyber-attacks, and vulnerability assessment are key components in addressing these threats (Mednikarov *et al*., 2020). A holistic approach to maritime cyber security management is recommended, with a focus on the increasing complexity, digitalization, and automation of systems (Mraković and Vojinović, 2019).

Silverajan and Vistiaho (2019) stated in their study that a prevalent security vulnerability currently identified in maritime vessels and operation systems is the simplicity of infiltration of malicious code and payloads, including but not limited to malware, ransomware, spyware, and viruses, into the critical systems of a ship. Injections of this nature manifest via malicious firmware updates, the introduction of a compromised device or sensor into the ship's network, or the utilization of infected removable media.

It has been discovered that certain onboard Voyage Data Recorders (VDR) are vulnerable to buffer overflows, common injection flaws, and faulty firmware update mechanisms (Söner *et al*., 2023). VDRs are supposed to be tamper-proof, but incidents have already occurred showing VDRs have been tampered with, in order to eliminate incriminating evidence of ship activity.

Ships are facing a growing number of cyber security risks associated with the compromise of their positioning and navigational systems, specifically through the manipulation or forgery of the Global Positioning System (GPS) signal. The act of spoofing a GPS signal entail manipulating the positioning systems installed on an unmanned vessel to perceive a forged signal, with the intention of causing inadvertent course corrections. GPS signal jamming is executed in a manner analogous to GPS signal deception, whereby the GPS receiver is obstructed from receiving any GPS signals or is duped into obtaining inaccurate location coordinates. At present, there is evidence suggesting that state-sponsored operations engage in deceptive GPS spoofing (Androjna and Perkovič, 2021).

Cyber security incidents in the maritime domain extend beyond the confines of ship-based systems. Recent reports have surfaced from various parts of the globe regarding ransomware and malware infections that specifically target ship navigational and control systems and ports (Meland *et al*., 2021). The NotPetya cyber-attack, which targeted the global systems of a shipping conglomerate, had far-reaching and consequential consequences that affected not only the organization but also the entire industry. Furthermore, it caused significant devastation to numerous interconnected enterprises operating in the manufacturing, logistics, and cargo handling sectors (Capano, 2021).

Karas (2023) stated that installing software, exchanging data, logging into systems, online banking operations, using data carriers these are just a few examples of activities during which a cyber-attack is possible. Accordingly, the most common types of cyber-attacks in maritime are phishing attacks, watering hole attacks, physical infiltrations, cyberpiracy, ransomware, integrated bridge system tampering, Automatic Identification System (AIS) spoofing, VDR tampering, GPS jamming.

In the literature, the studies directly related to maritime cyber incident analysis are limited. These are (Meland *et al*., 2021) and a preprint study Schwarz *et al*. (2021) However, rather than maritime industry, there are some studies related to cyber incident analysis in other sectors. For instance, Iaiani *et al*. (2021) aimed to provide a comprehensive overview of cyber-attacks on automated control systems in process facilities and share lessons learned from previous occurrences. Davis *et al*. (2009) examined the potential effects of cyber security incidents on firms that primarily operate online. It is tested for structural changes caused by widely reported cyber security incidents using web traffic time series for a representative collection of online firms. The findings consistently show that cyber security incidents have negligible effect on the structure of web traffic for the sample of online firms examined. Patterson *et al*. (2023) offer a fresh look at how organizations learn from incidents by methodically examining academic research on organizational learning from cyber security incidents and recommending additional research needs in this area. Kaneko *et al*. (2021) looked into an information security incident case called "AIST (National Institute of Advanced Industrial Science and Technology) report on unauthorized access to information systems," and attempted accident analysis with Causal Analysis using System Theory (CAST). They studied whether CAST, which is generally used for safety analysis, might be used to conduct cyber security analysis.

To the best of authors' knowledge, there is a gap for cyber incident analysis towards maritime industry in the literature. In this study, similar to Iaiani *et al*. (2021), a significant number of cyber-attacks infected the Operational Technologies (OT) systems and Information Technologies (IT) in maritime sector are analyzed by focusing on time trend, geographical distribution, impacts of the incidents, and nature of the cyber-attacks (attacker, intentional/accidental type, system infected). The analysis of a sub-set of more detailed incidents allowed the identification of the general steps of a cyber-attack on maritime systems, the main hacking techniques used by the attackers and the more common cyber security countermeasures applicable to the prevention of a cyber-attack.

3. METHODOLOGY

Data from the Marine Cyber-Attack Database (MCAD), the website containing cyber-attack data on the maritime industry created by NHL Stenden University of Applied Sciences, were analyzed. A total of 146 cyber-attacks took place between 2001 and 2023. These attacks were examined by dividing them into categories such as year, month, number of incidents, incident country, victim country, victim type, attack type. These categories are associated with each other and the number of incidents by years, the number of incidents by months, the comparison of incidents by months and years, the number of incidents by victim type, the number of incidents by countries, the number of cyber-attack attack types, the types of cyber-attacks on ships and ports are visualized and the findings are presented.

4. FINDINGS

The internet-based data shared by NHL Stenden University of Applied Sciences was analyzed in different categories. When cyber-attacks against the maritime sector from 2001 to 2023 are examined, it can be said that there is a generally rising trend until 2020 with the increase in technological developments (Figure 1). When the data is examined with the impact of the COVID epidemic on the world in 2020 and 2021, it is observed that there is an increase in cyber-attacks against the maritime sector. In the following years, it has been observed that there has been a decrease in these attacks with the increasing awareness in the sector, rules, published guidebooks and the measures taken by companies to protect their information systems. However, it should not be forgotten that with technological innovations, the number of successful cyber-attacks will increase due to the diversity of cyber-attacks and the lack of understanding of the cyber vulnerabilities of new systems.

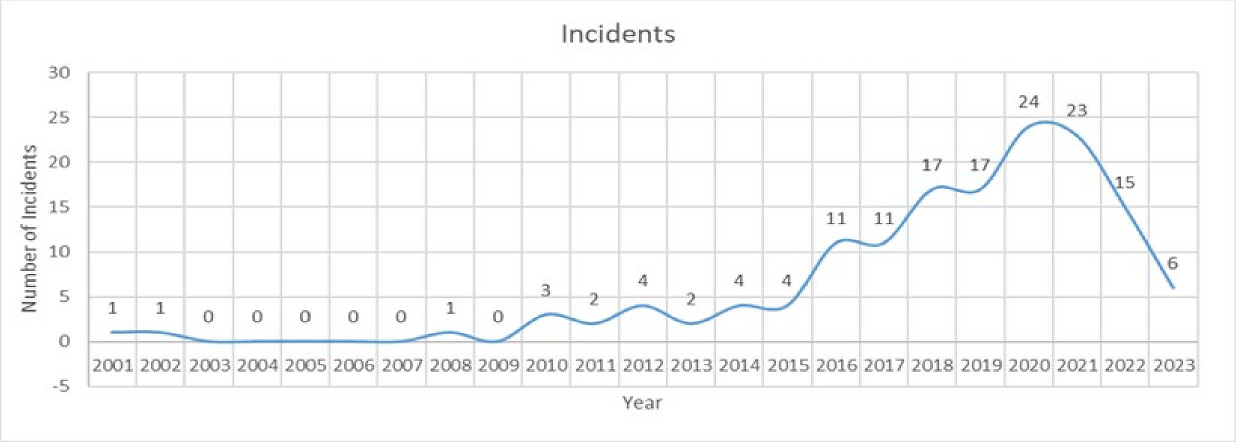

Figure 1. Cyber-attack incidents analysis to maritime sector between 2001 and 2023

When the cyber-attacks are analyzed by months, it can be said that the density of cyber-attacks is between 8 and 13 bands in Figure 2. However, cyber-attacks are more common in June, the beginning of summer, and September, the beginning of autumn, compared to other months. After June, especially in the months when people's holiday plans were more intense, cyber-attacks against the maritime sector showed a downward trend compared to other months, and with the beginning of September, this decrease ended and cyber-attacks increased.

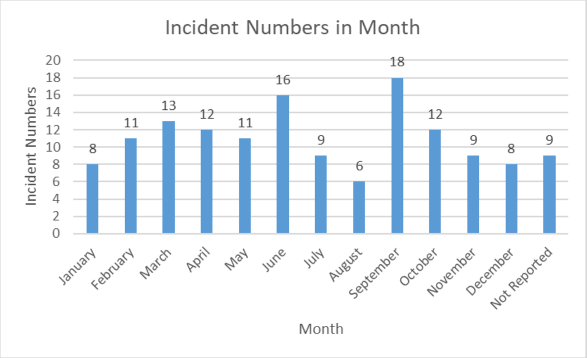

Figure 2. Number of cyber incidents by month from 2001 to 2023

When examined by year and month, as shown in Figure 3, the highest number of cyber-attacks against the maritime sector occurred in September 2020, 9 in total. One of these attacks took place against the CMA CGM company. The attackers notified the company that was exposed to the Ragnar Locker ransomware cyber-attack by sending an e-mail on September 27, 2020.

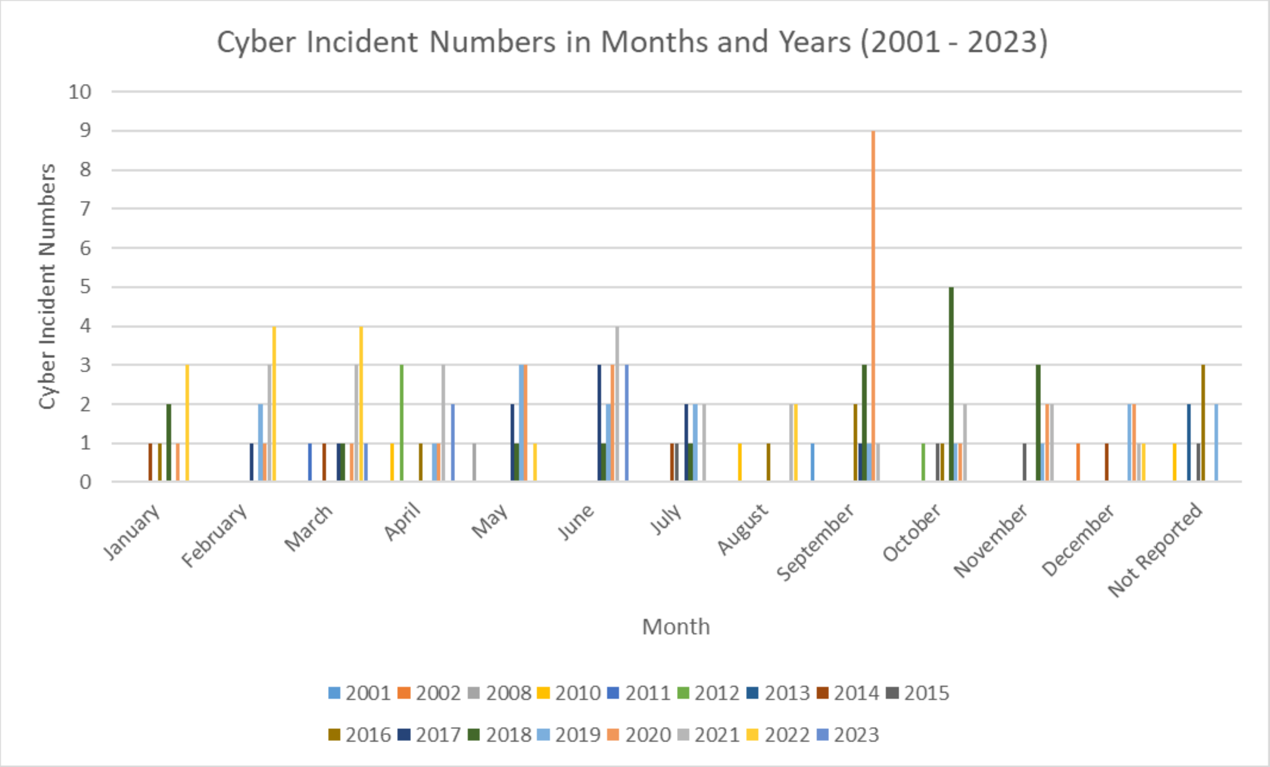

Figure 3. Maritime cyber incidents in months and years (2001-2023)

Cyber-attacks have affected many different stakeholders in the maritime industry. When the data is examined, it can be said that there is a more intense land-based attack on the maritime sector. However, we should not neglect the connection of ships with the land. In other words, it should not be forgotten that when a cyber-attack occurs against the maritime companies responsible for the ships in service, the ships they operate may also be affected by these attacks. At the same time, cyber-attacks on third parties working in cooperation with ships and shipping companies can affect both shipping companies and the ships they operate.

Maritime stakeholders exposed to cyber-attacks are shown in Figure 4. If we list the ones most affected by the attacks, vessels, shipping companies, ports, navy vessels, and shipbuilders are the parties most affected by cyber-attacks. Different actors of the maritime sector such as marine insurance, broker, salvage, offshore, coastguard, port authority are also affected by these attacks. These actors in the maritime sector are in close relationship with and influence each other. Therefore, it is one of the important cyber situational awareness that should not be forgotten that cyber-attacks on one of these actors may also affect other stakeholders.

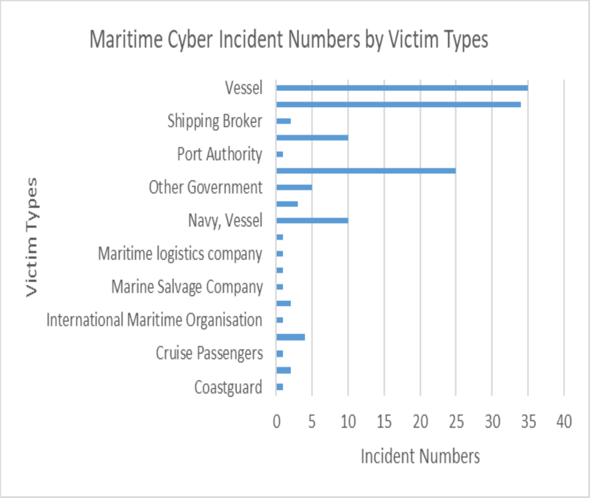

Figure 4. Maritime cyber incident numbers by victim types

In Figure 5, the analysis results of the maritime sector actors most affected by cyber-attacks are given according to their countries. In total, 43 countries were affected by maritime cyber-attacks. But the country most affected by these attacks is the USA. South Korea and the United Kingdom follow next. When the list is examined, it can be explained that actors in the world such as Russia-Ukraine, South Korea-North Korea, USA-Iran-China, who experience attacks and conflicts among themselves, are more affected by cyber-attacks than other countries.

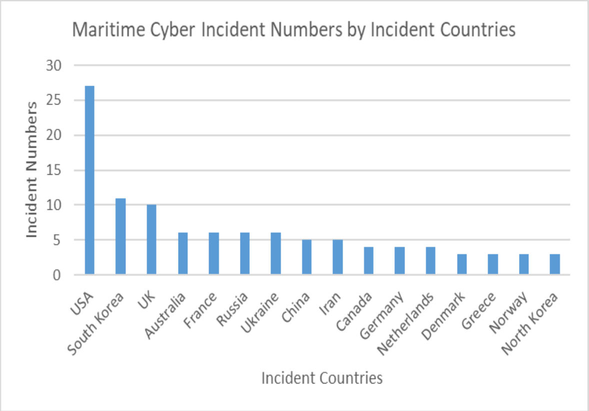

Figure 5. Maritime cyber incident numbers by countries where the incident took place

When we look at the types of cyber-attacks on the maritime industry, it is recorded that ransomware attacks occur the most (Figure 6). The maritime industry is one of the sectors where costs are intense, and planning and timing are important. The closure of the Suez Canal caused by the Ever given ship caused global shipping worth $10 billion to stop. It is obvious that the maritime industry will attract attackers because it is a sector that involves such high costs. Therefore, performing cyber-attacks on the information and operational systems of maritime industry stakeholders and demanding ransom for the systems to work again is a more popular type of cyber-attack among cyber attacker actors.

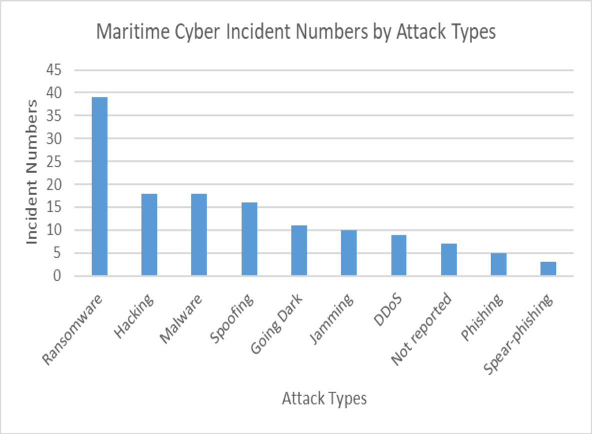

Figure 6. Maritime cyber incident numbers by cyber-attack types

When cyber-attacks against ships are analyzed, Spoofing, Jamming and Going Dark cyber-attacks lead the way. Spoofing attacks are carried out to manipulate AIS and GPS, including location and identities (Figure 7). The U.S. Maritime Administration sent a fairly ordinary safety advisory about GPS disruption in the Black Sea, nevertheless, the consequences were extensive. Commercial boats had substantial GPS errors, with several vessels displaying their location many miles onshore instead of being offshore. Several boats had similar problems, since their AIS systems displayed inaccurate vessel positions. The analysis indicates intentional manipulation of GPS signals, most likely achieved via the use of illegal jammers that are easily accessible on the internet. This occurrence highlights the susceptibility of GPS systems to manipulation, which raises issues over the safety of marine navigation and the availability of disruptive technologies.

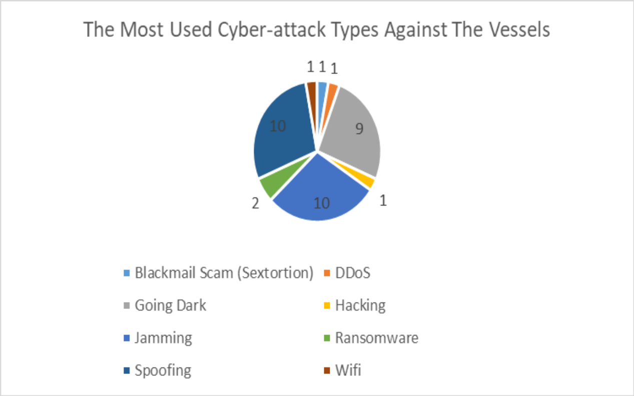

Figure 7. The most used cyber-attack types against the vessels

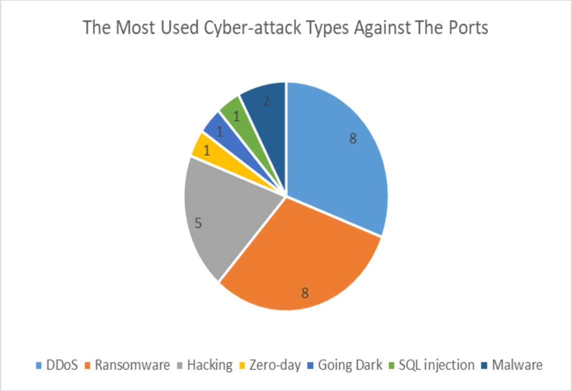

Figure 8. The most used cyber-attack types against the ports

In Figure 8, there are a total of 25 attacks against ports (One attack is both DDoS and malware). Ransomware, DDoS and Hacking cyber-attacks are the leading types of these attacks. Ports are one of the maritime infrastructures that play a critical role in carrying out the operations of ships. Therefore, attacks against them disrupt the operations of ships, disrupt global shipping, and endanger the maritime security of countries. In 2021, Transnet, the port operator in South Africa, invoked force majeure due to a ransomware assault that caused a complete shutdown of its IT systems and impacted container operations at many ports, including Durban, Cape Town, and Port Elizabeth in February 2022, a ransomware assault occurred at ports located in Germany, Belgium, and the Netherlands, resulting in the disruption of oil terminal operations and the incapacitation of port systems.

5. DISCUSSION

The analysis applied in the methodology section is reliable enough to make such specific conclusion because of several reasons - i.e. reliability and relevance of data source, transparency in comprehensiveness with which data has been analyzed, categorization & visualization techniques used, and its contribution for literature. MCAD an data source that is reliable and of utmost importance as this was created by NHL Stenden University of Applied Sciences in order to collect all information about the cyber-attacks in maritime domain. MCAD provides a detailed documentation of maritime cyber incidents between the years 2001 and up to 2023, therefore offering ample information on changes in cyber threats over time within the maritime sector. Database for maritime cyber-attacks is a major gap in the current academic literature, and it makes use of such a specialized and pertinent dataset render this study even more credible. Additionally, it being multi-dimensional approach i.e., to check not only type of incident but also the crime victim and country regional spread. These multi-dimensional categories enable the capture of both breadth and depth when considering cyber threats to shipping. This means that this paper does not simply reveal the top line or lay only superficial, toplining bare bones open for comparisons and contrasts about cyber-attack vulnerabilities in the critical infrastructure sector. By identifying and visualizing the data based on area like year, month, country-wise distribution of cyber-attack tells how these two different maritime sectors face potential attacks in their nature. Moreover, the categorization and breakdown of these threats over time offer a new understanding to maritime cyber risks that improves academic discourse as well as operations. This assists in the recognition of which actors are predominantly at higher risk by comparing incidents across various months, years and classifying it based on attack / victim type providing a good idea of its threat landscape. Decision-makers can use these visualizations to identify deep-rooted trends and advice their maritime cyber security policy.

This study on maritime cyber security incidents sheds lights upon some significant trends that reveal present day vulnerabilities and threats. Although improving operational efficiency, the growing digitalization of maritime systems has also given rise to more frequent and advanced cyber-attacks in this domain. The results confirm the gradual increase in cyber incidents seen over time, with a peak during COVID-19 and signs that an increased awareness of the threats including improved security measures has led to some decrease as well but also shows how maritime is challenged because of new form factors or cyber risk.

The research also contributes to such literature by adding the finer-grained geographical distribution of cyber-attacks and specific impact on various actors in the maritime industry, such as vessels, shipping companies, and ports. Indeed, attacks in countries such as the USA, South Korea, and the United Kingdom confirm scholarship done by scholars like Capano (2021), which shows the increase of geopolitical tension manifested in the cyber domain with state-sponsored cyber operations against critical maritime infrastructure.

These findings have important implications for stakeholders in the maritime industry. The study outlines the urgent need for closer international cooperation in the sharing of threat intelligence and actual development of uniform cyber security standards. Since the maritime systems are becoming increasingly interconnected, fragmented or isolated security methods will just not work. The patterns of the study will be important to inform future cyber defense strategies and policies, taking into consideration the seasonal peaks that cyber-attacks usually take place and the type of actors most targeted. The ability to learn from incidents in the past, coupled with adapting to the shifting threat landscape, determines the capacity to predict and prevent cyber-attacks.

6. CONCLUSION

The maritime sector, like all other sectors, is affected by digital transformations. As systems shift towards automation and their connections with each other over the network are increasing, the presence of cyber-attack actors in the maritime sector is mentioned. The source of finance, especially in the maritime sector, attracts cyber attackers. On the other hand, those who are attacked meet the demands of cyber attackers in order to avoid disruptions in their planning and loss of reputation in the sector.

In this study, cyber-attack data on the maritime sector between 2001 and 2023 from the Maritime Cyber-Attack Database (MCAD) provided by NHL Stenden University of Applied Sciences were examined in order to analyze cyber-attacks on the maritime sector. According to these investigations, cyber-attacks that started in 2001 reached their peak especially during the COVID19 pandemic. It shows a decreasing trend due to increasing awareness in the sector, regulations, guidebooks, and guidance from international organizations. When looked at by month, most attacks occur in September and June. September 2020 was the period when these attacks were most intense. When the victim groups are examined, ships, maritime companies and ports are the maritime sector actors that were most exposed to cyber-attacks. When examined in the victim countries category, the USA was most exposed to cyber-attacks. In the category of cyber-attack types, ransomware is at the top. While cyber-attacks against ships are spoofing and jamming, these attacks are observed as DDoS and ransomware in ports.

To sum up, many aspects have examined in order to understand the incentives behind cyber attackers and to guide stakeholders in the maritime sector towards implementing effective cyber security strategies and practices to prevent such cyber-attacks.

For further studies, it can be proposed correlation analyses between attack types and victim types, as well as time series analyses to further explore the trends in cyber-attacks over time. These enhancements would build on the existing methodology without undermining the conclusions drawn from the data thus far.

AUTHORSHIP CONTRIBUTION STATEMENT

Emre DÜZENLİ: Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing. **Gizem KAYİSOGLU:** Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing, Review and Editing, Visualization, Supervision. **Tayfun ACARER:** Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing, Review and Editing, Visualization, Supervision. **Pelin BOLAT:** Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing, Review and Editing, Visualization, Supervision. **Ayşe NAK:** Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing.

CONFLICT OF INTERESTS

The authors decelerate that they have no conflict of interest.

ETHICS COMMITTEE PERMISSION

No ethics committee permissions are required for this study.

FUNDING

This work was funded by Istanbul Technical University, Scientific Research Projects, General Research Project, which is titled as "Penetration Test Application and Analysis for ECDIS Cyber Security" with 44740 project code.

ORCID IDs

Emre DÜZENLİ:
https://orcid.org/0009-0009-5179-1627
Gizem KAYİSOGLU:
https://orcid.org/0000-0003-2730-9780
Tayfun ACARER:
https://orcid.org/0000-0003-2407-5552
Pelin BOLAT
https://orcid.org/0000-0003-4262-3612
Ayşe NAK:
https://orcid.org/0000-0003-2937-7007

5. REFERENCES

Androjna, A., Perkovič, M. (2021). Impact of spoofing of navigation systems on maritime situational awareness. *Transactions on Maritime Science*, 10(2): 361–373. doi:10.7225/toms.v10.n02.w08.

Ben Farah, M.A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., Bellekens, X. (2022). Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. *Information (Switzerland)*, 13(1). doi: 10.3390/info13010022.

Bernsmed, K., Frøystad, C., Meland, P.H., Nesheim, D.A., Rødseth, Ø.J. (2017). Visualizing Cyber Security Risks with Bow-Tie Diagrams. International Workshop on Graphical Models for Security, p. 38–56.

Bolat, P., Yuksel, G., Uygur, S. (2016). A Study for Understanding Cyber Security Awareness Among Turkish Seafarers. GMC2016 - II.Global Conference On Innovation In Marine Technology And The Future Of Maritime Transportation, p. 278–289.

Capano, D.E., Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk Industrial Cyber Security Pulse, (2021). Accessed Date: 08.05.2024, https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/ is retrieved.

Davis, G., Garcia, A., Zhang, W. (2009). Empirical Analysis of the Effects of Cyber Security Incidents. *Risk Analysis*, 29(9): 1304–1316. doi: 10.1111/j.1539-6924.2009.01245.x.

Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V. (2021). Analysis of Cybersecurity-related Incidents in the Process Industry. *Reliability Engineering & System Safety*, 209: 107485. doi: 10.1016/j.ress.2021.107485.

Kaneko, T., Yoshioka, N., Sasaki, R. (2021). Cyber-Security Incident Analysis by Causal Analysis using System Theory (CAST). 2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 806–815. doi: 10.1109/QRS-C55045.2021.00123.

Karas, A. (2023). Maritime Industry Cybersecurity: A Review of Contemporary Threats. *European Research Studies Journal*, 26(4): 921–930. doi: 10.35808/ersj/3336.

Kyriakides, H. Marine cyberattacks: Analysis of liability and IMO 2021, (2021). Accessed Date: 17.05.2024, https://www.legal500.com/developments/thought-leadership/marine-cyberattacks-analysis-of-liability-and-imo-2021/ is retrieved.

Mednikarov, B., Tsonev, Y., Lazarov, A. (2020). Analysis of Cybersecurity Issues in the Maritime Industry. *Information & Security: An International Journal*, 47(1): 27–43. doi: 10.11610/isij.4702.

Meland, P.H., Bernsmed, K., Wille, E., Rødseth, J., Nesheim, D.A. (2021). A retrospective analysis of maritime cyber security incidents. *TransNav*, 15(3): 519–530. doi: 10.12716/1001.15.03.04.

Mraković, I., Vojinović, R. (2019). Maritime cyber security analysis – How to reduce threats? *Transactions on Maritime Science*, 8(1): 132–139. doi: 10.7225/toms.v08.n01.013

NHL STENDEN University of Applied Science, (2001). Maritime Cyber Attack Database (MCAD), NHL Stenden University of Applied Science.

Patterson, C.M., Nurse, J.R.C., Franqueira, V.N.L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, 132: 103309. doi: 10.1016/j.cose.2023.103309.

Schwarz, M., Marx, M., Federrath, H. (2021). A Structured Analysis of Information Security Incidents in the Maritime Sector. ArXiv Preprint ArXiv:2112.06545.

Silverajan, B., Vistiaho, P. (2019). Enabling Cybersecurity Incident Reporting and Coordinated Handling for Maritime Sector. 2019 14th Asia Joint Conference on Information Security (AsiaJCIS), pp. 88–95. doi: 10.1109/AsiaJCIS.2019.000-1

Söner, Ö., Kayisoglu, G., Bolat, P., Tam, K. (2023). Cybersecurity risk assessment of VDR. *Journal of Navigation*, 1–18. doi: 10.1017/S0373463322000595.

Tam, K., Jones, K.D. (2019). Situational Awareness: Examining Factors that Affect Cyber-Risks in the Maritime Sector. *International Journal on Cyber Situational Awareness*, 4(1): 40–68. doi: 10.22619/ijcsa.2019.100125.