MEUJMAF

Mersin University Journal of Maritime Faculty

e-ISSN 2687-6612

December 2023 Volume: 5 Issue: 2

PUBLISHING BOARD

MERSİN UNIVERSITY JOURNAL OF MARITIME FACULTY (MEUJMAF)

Mersin University Journal of Maritime Faculty (MEUJMAF) is an international, scientific, and multidisciplinary journal which covers all fields of maritime sector. MEUJMAF publishes the articles in English and is being published 2 times a year. The Journal involves both experimental and theoretical studies on the subject area of Maritime Business Administration, Marine Transportation Engineering, Logistics, Supply Chain Management, Logistics Engineering, Naval Architecture Engineering, Marine Operations, Operations Research, Foreign Trade, Maritime Economics, Maritime History, International Trade, Marine Pollution and Port Management. MEUJMAF aims to contribute to the literature by publishing manuscripts at the highest scientific level in each abovementioned field and to convey the latest development in the science and technology to the related scientists and the readers.

AIM AND SOPE

Mersin University Journal of Maritime Faculty (MEUJMAF) is an international blind peer-reviewed open access journal, published twice a year. The Journal covers all fields of Maritime Business Administration, Marine Transportation Engineering, Logistics, Supply Chain Management, Logistics Engineering, Naval Architecture Engineering, Marine Operations, Operations Research, Foreign Trade, Maritime Economics, Maritime History, International Trade, Marine Pollution and Port Management.

PEER REVIEW PROCESS

All submissions will be scanned by iThenticate® to prevent plagiarism. Author(s) of the present study and the article about the ethical responsibilities that fit PUBLICATION ETHICS agree. Each author is responsible for the content of the article. Articles submitted for publication are priorly controlled via iThenticate® (Professional Plagiarism Prevention) program. If articles that are controlled by iThenticate® program identified as plagiarism or self-plagiarism with more than 25% manuscript will return to the author for appropriate citation and correction. All submitted manuscripts are read by the editorial staff. To save time for authors and peer-reviewers, only those papers that seem most likely to meet our editorial criteria are sent for formal review. Reviewer selection is critical to the publication process, and we base our choice on many factors, including expertise, reputation, specific recommendations and our own previous experience of a reviewer's characteristics. For instance, we avoid using people who are slow, careless or do not provide reasoning for their views, whether harsh or lenient. All submissions will be double blind peer reviewed. All papers are expected to have original content. They should not have been previously published and it should not be under review. Prior to the sending out to referees, editors check that the paper aim and scope of the journal. The journal seeks minimum three independent referees. All submissions are subject to a double blind peer review; if two of referees gives a negative feedback on a paper, the paper is being rejected. If two of referees gives a positive feedback on a paper and one referee negative, the editor can be decide whether accept or reject. All submitted papers and referee reports are archived by journal Submissions whether they are published or not are not returned. Authors who want to give up publishing their paper in MEUJMAF after the submission have to apply to the editorial board in written. Authors are responsible from the writing quality of their papers. MEUJMAF journal will not pay any copyright fee to authors. A signed Copyright Assignment Form has to be submitted together with the paper.

PUBLICATION ETHICS

Our publication ethics and publication malpractice statement is mainly based on the Code of Conduct and Best-Practice Guidelines for Journal Editors Committee on Publication Ethics (COPE). (2011, March 7). Code of Conduct and Best-Practice Guidelines for Journal Editors. Retrieved from http://publicationethics.org/files/Code%20of%20Conduct_2.pdf

PUBLICATION FREQUENCY

The MEUJMAF accepts the articles in English and is being published 2 times (December and June) a year.

CORRESPONDENCE ADDRESS

Journal Contact: meujmaf@mersin.edu.tr

CONTENTS

Volume 5 – Issue 2

ARTICLES

Mersin University Journal of Maritime Faculty

Mersin University Journal of Maritime Faculty (MEUJMAF)
Vol. 5, Issue 2, pp. 22-36, December 2023
e-ISSN 2687-6612, Türkiye
DOI: 10.47512/meujmaf.1370274
Review Article

THE ROLE OF CYBER SITUATIONAL AWARENESS OF HUMANS IN SOCIAL ENGINEERING CYBER ATTACKS ON THE MARITIME DOMAIN

Cihat AŞAN *[1]

[1] Piri Reis University, Maritime Faculty, Maritime Transportation and Management Department, Tuzla, Istanbul, Türkiye
ORCID ID 0000-0003-3674-6616
e-mail: casan@pirireis.edu.tr

* Corresponding Author

Received: 02/10/2023 Accepted: 12/12/2023

ABSTRACT

Through technological advancements, the expanding proportion of maritime transportation on a global scale is becoming faster, more automated, more digital, and ultimately more cyber-space. In particular, the Industrial Revolution 4.0 has brought real-time digital integration of stakeholders in the maritime industry, both on land and at sea, into cyberspace. However, the scope of life and property protection at sea has expanded with the participation of the cyber environment as well as the physical environment. The human factor plays a leading role in ensuring the security of both the physical and cyber environment. In parallel, the main target of hackers who try to gain profit by violating the security environment is the person who does not have sufficient situational awareness of cyber security and can be called the weakest link in the chain. In this study, as main goal, the role of the situational awareness of the employees in the past cyber-attacks on the maritime industry was examined, and a perspective on the measures to be taken was presented. To achieve this research goal, the study utilized the snowballing technique to access literature, which helped uncover additional relevant resources not initially detected. This was followed by a systematic analysis of the collected literature. An analysis of attacks conducted since 2010 revealed that 76% of them utilized social engineering methods, such as phishing, malware, and ransomware. These attackers appear to exploit the maritime industry's insufficient cybersecurity awareness among its employees and the lack of a comprehensive understanding of cybersecurity within the industry.

Keywords: *Maritime industry, Cyber security, Cyber-attack, Situational awareness*

1. INTRODUCTION

Throughout history, changes in production have shaped societies and lifestyles, creating new needs. This transformation is driven by economic demands, supply and demand dynamics, and international trade. These advancements have fostered and advanced capitalism, often labeled as the "industrial revolution" in academic discourse. Industry 4.0 represents the convergence of information technology and manufacturing, affecting multiple sectors, including the maritime industry.

Maritime transportation is an indispensable means of importing and exporting various commodities in the contemporary era. The advancement of technology has led to the progression of the technical structure of ships through the implementation of digitalization, integration, and automation systems. Developments that have been brought into the scene by Industry 4.0 have introduced concepts such as smart ports, intelligent vessels, and automated operations in maritime operations. Regarding the maritime domain in general, although all activities such as port administrations, management of ships, class organizations, ship agents, equipment manufacturers, ports, terminals, and logistic activities are based on the computer system, this technological change also includes negative aspects. Besides creating opportunities for maritime companies and commercial stakeholders, technological developments have also provided opportunities for crime actors by making the sector vulnerable to cyber-attacks (Fitton et al., 2015). With the rise of cyber-attacks, it is anticipated that in the future these attacks have the potential to seriously disrupt critical infrastructure. It is evident that the maritime industry conducts more cost-effective operations in line with technological advancements. However, the threat level posed by cybersecurity risks accompanying these technological advancements is crucial for security. In this context, a critical question arises: "What is the role of employees in the damage caused to the maritime industry by these emerging cybersecurity threats?"

Based on this research question study focused on human behaviors in cybersecurity. Hackers may employ social engineering techniques to obtain access to an organization's network by taking advantage of interpersonal relationships or social abilities (CISA-US, 2020). These human manipulations, which are utilized by hackers, have progressed from the stage where they try to convince company users to reveal their accounts to the stage where they use social networking sites to undertake reconnaissance to get relevant information about an enterprise (Algarni et al., 2013). As a part of this process, it is essential to recognize that cyber security is a human behavior issue, and not exclusively a matter for the Information Technology (IT) departments (Alcaide and Llave, 2020). This is supported by data that shows that human conduct, whether done purposefully or accidentally, is a common source of cyber mishaps (Futurenautics Maritime-KVH and Intelsat., 2018). Despite this, the primary factors that lead to cyber-attacks are incredibly nuanced, and in the context of maritime cyber security, people may be both an indispensable resource and a potential threat (Hareide et al., 2018).

The main goal of this study is to demonstrate the role of employees' situational awareness of cyber security by conducting a state-of-the-art literature review of past cyber-attacks against the maritime domain. For this purpose, the resources of the resources were reached with the snowballing technique (Wohlin, 2014) so that the work was deepened by providing access to the resources that were not detected at the first stage, but which were related to the subject. Under the auspices of Okoli processes, a literature review was undertaken based on four primary steps: planning, selection, extraction, and implementation (Okoli, 2015). As a result of this review, findings have been presented, and while the role of cyber risk perception and situational awareness of humans in social engineering cyber-attacks on the maritime domain has been put forward as a conclusion, ideas for improving this awareness have been put forward as recommendations.

The conclusion stems from the analysis of cyberattacks conducted since 2010 in the maritime domain, revealing that 76% of them employed social engineering methods. Consequently, the primary outcome of the study indicates a substantial deficiency in employees' cybersecurity awareness, necessitating substantial and altruistic endeavors for improvement.

The major importance of the study is highlighting that the concept of cybersecurity in the maritime industry is not the responsibility of a specific group; especially, it underscores the significance of the human factor and how it represents both a crucial aspect and a weak link. In light of studies like this one, it is essential to conduct more comprehensive research to prioritize measures related to human behavior in cybersecurity.

2. LITERATURE REVIEW

Some research on cybersecurity has focused on examining situational awareness, which may include cognitive studies (D'Amico et al., 2005; Kokar and Endsley, 2012; Mahoney et al., 2010; McNeese et al., 2012). Other research has looked at behavioral elements to gain a better understanding of general cybersecurity awareness in organizations (Bada et al., 2019; Lebek et al., 2014; Pfleeger and Caputo, 2012).

The study of Farah et al., (2022), presents a taxonomy of cyber-attacks focusing on the maritime industry. has been provided and an analysis of cyber-security frameworks has been offered. In their study, Larsen and Lund, (2021) present a method for examining cyber risk perception through the use of acknowledged psychological models and give a current research overview of the topic in the context of the maritime realm.

To investigate the correlation between Cyber Curiosity and Situational Awareness, and their impact on cyber risk in organizations, Perez, (2019) created an interactive web-based site survey. The study was conducted with a total of 174 Information System (IS) users, comprising 120 maritime and 54 shoreside users. The information obtained was subjected to analysis to ascertain whether there exist any noteworthy variances in the degrees of Cyber Situational Awareness and Cyber Curiosity among IS users who operate in maritime and shoreside settings. Additionally, the study sought to examine how their respective positions within the established Cyber Risk classification scheme impact these constructs.

Mraković and Vojinović, (2019a) address some of the most significant challenges facing the maritime industry from the point of view of cyber security and offer some suggestions for resolving or mitigating those challenges.

Due to the growing awareness among hackers of the cyber vulnerabilities present in the maritime domain, and with their assessment of the inadequacy of existing risk assessment tools in addressing the distinct character of maritime cyber threats, Tam and Jones, (2019) put forward a model-based framework for risk assessment. This framework combines both cyber and maritime factors to better assess the risks faced by the maritime industry.

Bolat and Kayışoğlu, (2019) investigated cybersecurity awareness in the maritime industry, utilizing the Turkish Maritime Sector as a case study. Employing Structural Equation Modeling the study emphasizes the significant role of education in enhancing cybersecurity awareness. It also highlights the impact of cybersecurity incidents on both awareness and behavior, establishing a noteworthy correlation between maritime cybersecurity awareness and the adoption of secure user behavior. Importantly, the study suggests that factors such as rules, policies, and information sharing have limited influence on cybersecurity awareness and the development of secure employee behavior.

3. METHODOLOGY

With the progression of technology, the proliferation of Industry 4.0 in the Maritime domain has entailed the emergence of cyber security concerns. The exploitation of the vulnerabilities inherent in human behavior, commonly referred to as social engineering, is a significant factor in the success of cyber-attacks. The absence of cognizance about social engineering attacks can make an organization more susceptible to cyber-attacks. To fulfill the objective of the study, the literature was initially accessed utilizing the snowballing technique (Wohlin, 2014), thereby allowing for a greater understanding of the topic at hand by providing access to resources that were not initially detected, yet still associated with the subject. The literature was subjected to a systematic analysis utilizing the Okoli processes, as outlined in Figure 1.

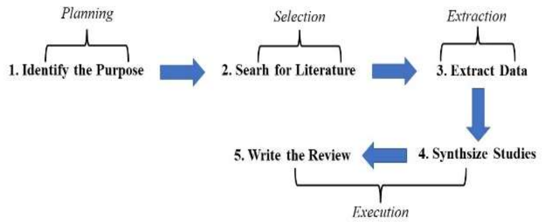


Fig. 1. Methodology for constructing the literature review (Okoli, 2015)

During the 'Planning' stage, the purpose and scope of the scan were established as cyberattacks that had been perpetrated directly against the maritime sector since 2010, with successful results and significant consequences. In the "Selection" phase, the literature relevant to this purpose was identified through reports and existing studies. In the "Extraction" phase, the targets of the listed cyber-attacks were scrutinized, and during the "Execution" phase, the evaluation of which of these targets were executed through ransomware/malware exploiting the situational awareness deficiency of the staff within the ambit of social engineering was completed.

4. CYBER RISKS IN THE MARITIME DOMAIN

The Industrial Revolutions played a pivotal role in driving industrialization, accelerating economic growth, and causing significant shifts in societal structures. Presently, modern industrial production technologies continue to bring about revolutionary changes, with a growing impact on the global economy. We are now in the era of Industry 4.0, often termed the fourth industrial revolution or the digitization period. In the maritime industry, Industry 4.0 technologies are actively employed to enhance the efficiency, safety, and sustainability of ships and their operations. This transformation involves the integration of advanced technologies into ship design, construction, and operation, resulting in a more efficient, secure, and sustainable maritime sector. However, the challenge of safeguarding against cyber threats has emerged as a significant obstacle for companies adopting the Industry 4.0 framework to maintain their competitive edge.

The management of cybersecurity within Industry 4.0 is a pertinent and evolving subject in contemporary academic literature. While various methodological solutions have been proposed to address cybersecurity concerns in the context of Industry 4.0, there is a gap in these solutions, as they do not adequately establish links between critical assets requiring protection against cyber-attacks and the subsequent impacts on business operations, nor do they provide a measurable metric for assessing these effects. (Corallo et al., 2020).

With Industry 4.0, the concept of risk management against cyber threats has also found its place on the agenda. "Cyber risk" refers to the potential harm stemming from the manipulation of cyberspace by adversaries, involving threat assessment, vulnerability evaluation, and an understanding of the consequences. In contrast to "cyber-attacks," which are specific offensive actions, "cyber risk" takes a more holistic view, encompassing the broader landscape of vulnerabilities, threats, and potential impacts, along with measures to manage and respond to digital threats. This manipulation may target various components of cyberspace, including computer systems, services, embedded processors/controllers, and data that is either while in stored or in process. When examining the cyber threats that merchant vessels face, it is advantageous to classify their systems into two distinct categories: Onboard Operational Technology (OT) systems are cyber-physical systems that interact with their environment by controlling physical components and processes. This includes handling cargo frameworks, bridge facilities, propulsion and machinery executives, and power management systems. IT systems, on the other hand, refer to a range of functions such as data management, access control, passenger management, networking, executive and crew assistance, communication, and ship-to-shore connections. In sum, merchant ships and their management must be aware of the risks posed by both OT systems and IT systems. (Refsdal et al., 2015), (IMO, 2017).

In particular, the scope of such risks will increase in the possibility of the spread of passenger and cargo transportation without a ship crew (autonomous. ships) in the coming years. To engage in maritime activities that involve such as Global Positioning Systems (GPS), autonomous technology, physical safety sensors, digital certificates, cargo tracking, electronic navigational components, automatic identification systems, and record keeping it is imperative to utilize secure computers and an encrypted internet connection. All of these systems are vulnerable to cyberattacks whenever they are connected to the internet. To give an example of the damages that can occur with various malware attacks; damage to sensitive cargoes, cargo hijacking, delay, loss, damage, damage to transportation facilities (port, marina, etc.), the collision of ships, accident of port operators, alteration or destruction of information in the bill of ladings and cargo manifests, seizure of trade secrets, commercial reputation injury, etc. Because data has value like capital in cyberspace, data protection is also important. In addition to company data, personal data is also at risk from cyber dangers. Although the results of cyber-attacks are generally economic damage, they have a high potential to harm people and the environment. Accidents that may result in injury or death may occur due to the steering of ships for malicious purposes, or the deactivation or steering of machinery. Again, as a result of malicious cyber interventions environmental damage is inevitable via physical damage such as collision or grounding and the leakage of the ship's fuel or harmful chemicals and cargoes.

4.1. Types of Cyber Attacks

According to the studies that are cited in the following paragraphs, the most significant maritime cyber challenges present themselves in the following forms:

4.1.1. Spear-phishing: It is the most prevalent cyber incident type. Among the most common attacks is spear-phishing, which uses emails containing suspicious links to obtain unauthorized access. (Clark, 2018; Mraković and Vojinović, 2019c). There are two primary classifications of attacks: social engineering and malware-based. Social engineering relies on exploiting human curiosity or carrying out illicit activities (Jensen, 2015), while malware-based attacks utilize malicious software (Gupta et al., 2017). With regards to social engineering, attackers endeavor to cause harm using electronic mail which might appear innocuous upon first assessment, or by means of bogus websites. Conversely, malware phishing employs malicious programs that are installed on the user's computer. Maritime vessels are commonly subjected to this type of security threat by way of electronic mail. E-mail communication typically includes a hyperlink to a false website, where the individual may unknowingly enter confidential information, for example, their username and password, due to either a lack of attention or understanding. Typically, when personnel are overworked and inattentive to the information contained within emails or the associated hyperlinks, this occurs. Despite the prevalence of spear-phishing attacks, port managers are reticent to report incidences, due to the sensitivity of the maritime sector, as breaches can have adverse implications not only for the confidentiality of individuals but also for the economic ties between nations. (Mraković and Vojinović, 2019c).

4.1.2. Ransomware: Malicious software of this type is commonly referred to as malware. It is often the case that an e-mail that appears innocuous can create significant disruption. Ransomware is typically presented in the form of Portable Document Format (PDF) or compressed (ZIP) files, which are attached to electronic mail messages. The initiation of the malware may lead to a denial of access to documents or the system as a consequence of opening these files, posing a danger to the system. The resolution would involve reimbursing ransom to successfully regain access to files or systems. (Mraković and Vojinović, 2019c).

4.1.3. Distributed Denial of Service (DDoS): DDoS attacks are regarded as criminal. The port IT systems have been rendered inaccessible due to the inundation of the network with an excessive amount of traffic, thus obstructing access to its sites. (Kessler and Uk, n.d.).

4.1.4. Port Scanning: Attackers ascertain the most susceptible network ports by utilizing the traditional approach of scanning. The objective is to ascertain the condition of services, determine the best method to gain access to databases, and recognize which users are cognizant of services. At the most sophisticated level, the perpetrator utilizes IP fragmentation to perplex the firewall, thus allowing the packet filters to be circumvented. Another approach is based on interrogating a port at the Transport Layer of the Open Systems Interconnection (OSI) Model, to scan IP addresses through a trial of multiple protocols and other ports. The test models employed by a hacker are created randomly (Hindy et al., 2021).

4.1.5. Supply chain: Attacks on the supply chain can be focused on exploiting the weakest element within the entirety of the end-to-end network to create disruption (Lam and Bai, 2016). The successful facilitation of global shipping and transportation of cargo from origin to concluding destination relies upon essential processes and stakeholders for container tracking, confirmation, and intercontinental permissions. An illustrative instance of a deleterious effect of an attack is the alteration of the destination of a container, which necessitates expertise in the supply chain and the susceptibilities within it, to adjust critical data. (Mraković and Vojinović, 2019c).

4.1.6. Man in the middle (MITM/MIM): This kind of malware exploits weaknesses in the SSL/TSL protocol, which facilitates communication between two networks (Čekerevac et al., 2017; Mallik et al., 2019). In such circumstances, the downloading of significant data takes place while users rarely can detect it.

4.1.7. Data theft: In many cases, it is not detected until after an extended period or is not acknowledged at all. Unauthorized data duplication or downloading is occurring. Engagement in criminal endeavors through the utilization of ransomware and malware, with illicit access leading to both data theft and data erasure to disguise evidence or inflict immense damage to corporate entities. (Borazjani, 2017).

4.2. Human Factor in Cyber Security

The end user plays a crucial part in cybersecurity by helping to guard against, identify, and counteract cyberattacks. Cybersecurity is a user-centric notion that necessitates the implementation of secure behavior to protect against online vulnerabilities and assaults. Users' awareness of the importance of cyber security to their personal and professional lives has emerged as a major obstacle to the continued success of digital information exchange. End users are workers, so they should be made aware of the importance of their role in maintaining the safety of the cyber-physical system and safeguarding the data that passes through it. Cyberattacks can occur due to human error, such as the use of weak passwords, the opening of unfamiliar e-mail files, or the disregarding of dangers brought about by wireless networks and mobile devices at work. Therefore, education is the first line of protection. (NSI, 2017). In addition, fostering a culture of cybersecurity consciousness and encouraging a proactive approach to threat identification and reporting should be integrated into the overall strategy to address the human factor. This involves promoting vigilance, clear reporting channels for suspicious activities, and ongoing awareness campaigns to ensure that cybersecurity remains a collective responsibility within the organization.

Because the human component has become such an essential concern to ensure cybersecurity, the businesses that are directly connected to the human element may be exposed to a significantly higher level of risk than the other sectors. Given these circumstances, the maritime transportation industry becomes a major hub from the point of view of cybersecurity. This is due to the fact that 90% of maritime accidents have happened due to human-related mistakes. When incidents and penetration tests involving cybersecurity in the maritime industry are evaluated, it is clear that a dearth of knowledge and an inability to adopt safe behavior are significant contributors to the frequency of cybersecurity incidents. It is clear from looking at responsible individuals who are involved in connected cyberspace that they are unaware of the security procedures aimed at the system (ENISA, 2011b; S. de Vleeschhouwer, 2017).

Consequently, maritime transportation is an area with a high level of cybersecurity risk and a low level of cybersecurity awareness. This approach was also supported by the European Network and Information Security Agency, which outlined seven significant gaps in maritime cybersecurity: “Low awareness and focus, the complex structure of Maritime systems, absence of holistic management approach in a national and international context in the maritime field, inadequacies related to the security of cyberspace in maritime regulations, no holistic understanding of cybersecurity, lack of economic incentives and initiatives for work to increase the cybersecurity in the maritime sector, lack of incentives to motivate work” (ENISA, 2011b).

4.3. Cyber-attack incidents in the maritime domain

4.3.1. Year 2010:

Malware on the offshore rig: Malicious computer software overpowered a drilling rig while it was at sea after departing from its South Korean construction location to Brazil. The blowout preventer, a crucial piece of safety equipment, was controlled by computers that were corrupted by the malware because it had expanded so widely throughout the rig's systems[1]. This was one of several rigs that experienced similar issues after their construction. Even computers on offshore oil platforms that are not linked to the Internet and were not designed to communicate with the Web have been infected by malware. Users who engage with the computers while inadvertently transporting problematic files cause issues frequently. Links in malicious emails or malicious webpages can contain links that download those files onto a computer, where they can then attach to USB devices or propagate over a network. Source: (Shauk, 2013)

Hacking of a Greek shipping company: A Greek shipping company was the target of multiple successful piracy assaults in the Gulf of Aden over two years. This was because local pirates employed hackers to gain access to the company's headquarters and identify the ships that were the most susceptible to attack, as well as route itineraries. Hackers were able to access the information technology systems of the business by using the wireless equipment that had been installed in the company's buildings. (Kapalidis, 2020)

4.3.2. Year 2011:

IRISL: The servers of the Iranian Shipping Corporation IRISL (Islamic Republic of Iran Shipping Lines) were compromised as a result of a cyber-attack, resulting in the loss of data pertaining to rates, loading, dispatch, and location. Consequently, the location of numerous cargo containers remained unknown, and an undisclosed quantity of financial losses resulted. Sources: (Kapalidis, 2020; Torbati and Saul, 2012)

4.3.3. Year 2011-2013:

Port of Antwerp: A criminal organization utilized the port of Antwerp to transport large quantities of narcotics from South America disguised as bananas. To accomplish this, the organization employed a group of Belgian hackers who compromised the management systems of two

[1] According to Michael Van Gemert, who manages systems and controls for Lloyd's Register Drilling Integrity Services, an offshore inspection company that was informed about the incident, the rig encountered malware and had to be shut down for several days during its journey from Korea to Latin America in 2010.

terminals in the port. The infiltration allowed the criminal organization to locate every container prior to the arrival of the actual client to collect it. Sources: (Kapalidis, 2020; Nguyen, 2018; Walker and Spencer, n.d.)

Saudi Aramco, Oil and Gas Operator: During the month of Ramadan in 2012, the main Saudi Arabian state-owned oil and gas corporation, Saudi Aramco, which supplies 10% of the world's oil, suffered a cyberattack. A company employee opened a phishing mail containing an infected link. According to Aramco's vice president of corporate planning, Abdullah al-Saadan, the primary objective of this attack was to prevent the flow of oil and gas to both domestic and international markets. Due to this attack, the company failed to send or receive financial transfers or contracts, as well as process payments, compelling it to cease operations and close its internal corporate. Moreover, the negative effect resulting from the attack had a significant impact on the company's supply chain, particularly in maritime transportation. As a result, it became clear that cyberattacks could have far-reaching consequences beyond the immediate financial damage they cause. Sources: (Reuters, 2012)

Danish Maritime Authority: In 2012, the Danish Maritime Authority was targeted by malware encoded in a PDF file. Before being found in 2014, the virus had expanded throughout the Maritime Authority's network and into Danish government organizations. A large majority of cyberattacks are the result of human activity. Authorized users make poor password decisions, click on harmful links, open email files containing malevolent code, misplace their computers, tablets, and phones, and have their usernames and passwords collected by a growing number of phishing scammers. Source: (Linton, 2016)

4.3.4. Year 2015:

Mobile Offshore Drilling Unit (MODU): In 2015, the US Coast Guard reported a case in which offshore oil employees carried infected laptops and USB drives aboard a MODU. The accidentally transmitted malware disrupted computer networks by downloading adult and unlawful music files directly. The malware disabled the dynamic positioning and thruster signals, causing the MODU to drift away from the well site. As stated by Nguyen, (2018):

"This incident is another example of a non-existent 'cyberculture'. The incident highlights the disastrous effects that such an attack on an offshore critical infrastructure, or a ship, could have on the environment. A case that affected both the human factor and the infrastructure and illustrated the necessity for effective cyber training for maritime professionals, once again".

Sources: (Athens Group Services, 2019; Kapalidis, 2020; Nguyen, 2018)

4.3.5. Year 2016:

South Korean fishing boats: After GPS signals were disrupted, which also made it difficult to locate fishing nets at sea, hundreds of South Korean fishing vessels were forced to return in early 2016. South Korean authorities said this was due to the jamming of GPS signals. The occurrence has been attributed to North Korea, but there was no evidence to support this claim. Source: (Kim and Saul, 2016)

4.3.6. Year 2017:

Clarksons incident: Clarksons is one of the largest shipbrokers in the globe. According to the company's official press release, unauthorized access was attained through a solitary, isolated user account in November 2017. Following the stealing of sensitive information, the stock value decreased by 5% immediately. It demonstrates the significance of developing "cyberculture" for the most vital pillar of cyber resilience, the human element. It highlights the need for effective cybersecurity training for all maritime professionals. Companies should revise their access and administration rights by the "need-to-know" principle, limiting them to only the necessary personnel and closely monitoring them all. Sources: (Nguyen, 2018), (Kapalidis, 2020)

Maller Maersk: A significant maritime firm, A.P. Moller-Maersk, experienced a significant business interruption cyber incident in June 2017. The notPetya malware was brought to the company's terminal in Ukraine by a claimed state-drive assault. NotPetya caused global disruptions that persisted for weeks. According to the Chief Information Security Officer of Maersk, the event began with the infection of a single user's workstation and spread rapidly within seven minutes (Parizo, 2019; Progoulakis et al., 2021). As many as 76 of the company's port facilities around the world were affected by the virus, including important ones like Rotterdam, Los Angeles, Mumbai, and Auckland.

Sources: (Cimpanu, 2018b; Maritime Executive, 2020c; Mcquade, 2018; Nguyen, 2018)

Subcontractors of the US Navy: Hackers from China are suspected of obtaining information from companies that provide services to the United States Navy. In addition, it is believed that 27 Universities in the United States have been targeted in an operation to acquire research data associated with maritime technology. Sources: (Lubold and Volz, 2018; Volz, 2019).

4.3.7. Year 2018:

Port of Barcelona: The Port of Barcelona reports a cyberattack in 2018, which turned out to be a "Ryuk" ransomware infection. Only internal IT systems were harmed by the attack, not ship traffic. When ransomware got into a computer, it messed up the camera and access control systems and caused important process control tracking systems to stop working. A malicious email sent to a worker at the marine center was the point of entry. "Once an employee clicked on the malicious link in the email, the ransomware allowed a threat actor to access important enterprise IT network files and encrypt them, making it impossible for the facility to access important files," the agency said. Sources: (Cimpanu, 2019; Safety4sea, 2018)

Port of San Diego: Five days after the aforementioned occurrence in Barcelona, the Port of San Diego reports serious disruptions to its IT systems. This was another Ryuk ransomware infection, and its effects are limited to the port's local operations. It was subsequently disclosed that both incidents were caused by the same Ryuk ransomware. Sources: (Cimpanu, 2019; Safety4sea, 2018)

Gold Galleon: A monetarily driven Nigerian threat organization known as "Gold Galleon" is engaged in business email compromise (BEC) and business email spoofing (BES) scams. The Group stole at least $3.9 million US dollars from marine shipping companies and their clients between June 2017 and January 2018. BEC is a type of social engineering plan in which threat actors obtain entry to a company's email account. The attackers typically use spear phishing emails with malicious payloads attached to capture the email passwords of people in charge of business operations. Sources: (Secureworks, 2018)

COSCO: A cyberattack was launched against China Ocean Shipping Company, also known as COSCO, which resulted in significant disruptions in the network operations of their US office. For a period of five days, correspondence via email and the network telephone was disrupted. Emails sent within the company suggest that the incident was caused by an infestation with ransomware. Sources: (Cimpanu, 2019; Interpol, 2020)

SAIPEM attack: Saipem, an Italian subsea engineering and energy services company, disclosed that it had detected a hacking attempt on its Middle Eastern server systems. About 400 of Saipem's servers, predominantly those located in Middle Eastern nations, were affected by the attack, but not the company's primary servers in Europe, according to company officials. The suspected origin of the hacking endeavor is India. The company had backups of all the afflicted data, so no information was lost irreversibly. Saipem has found no evidence to suggest that any data was taken. Source: (The Maritime Executive, 2020)

GPS jamming: In northern Norway, there have been numerous reports of GPS interference throughout the course of 2018 and 2019. The disturbance has had some effect on maritime traffic, but fortunately, the situation could have been much worse had it not been prevented. Sources: (Meland et al., 2021; The Norwegian National Security Authority (NSM), 2020)

4.3.8. Year 2019:

Large ship en route to New York: In February 2019, a large ship that was sailing towards New York City reported a serious cyber-attack on its onboard network to the US Coast Guard. An incident-response team led by the Coast Guard found out that the ship's systems had been infected with malware, causing severe damage to their functionality. A warning was issued to commercial vessels urging them to improve their cybersecurity by splitting shipboard networks, enforcing per-user passwords and tasks, implementing fundamental security measures, and patching regularly. Source: (Lemos, 2019)

Undisclosed port in the USA: The Ryuk ransomware has attacked a port in the United States that has not been identified. Because of the infection, CCTV cameras, access control systems, and essential process monitoring were rendered inoperable. The infection was spread through an attachment in a phishing email. Source: (Cimpanu, 2019)

James Fisher & Sons (JFS): A maritime services provider JFS, located in the United Kingdom, has announced that it has become the target of a cyber-attack and has made the decision to temporarily disable its digital systems as a preventative measure. The irony of the situation is that the official revelation of the data compromise has caused a 7% drop in the price of the company's shares. Officials from the JFS have stated, under the condition of confidentiality, that the assault was a ransomware variation that prevented access to the files. Source: (Goud, 2019)

Undisclosed US pipeline operator: Due to being infected with Ryuk ransomware, a natural gas compression facility belonging to an unnamed US pipeline provider is forced to go offline for two days. Phishing emails were used in the assault, and both IT and operational technology systems were compromised as a result. Sources: (Buurma and Sebenius, 2020; Dragos, 2020)

A tanker in Finland: Ransomware compromises the administration computer of a tanker that is located in the vicinity of the harbor of Naantali in Finland. Additionally, the archival drive is formatted. It has been determined that the Remote Desktop Protocol (RDP), a USB device, or an email attachment are all potential entry points for an attack. Four months later, in the vicinity of the same harbor, the same vessel becomes infested once more. Source:(Meland et al., 2021).

Hermes 2.1.: Two vessels belonging to the same proprietor have been infiltrated by the Hermes 2.1 ransomware. The intrusion was propagated through a Word document with macro capabilities embedded in an email, resulting in the compromise of multiple computers on the administrative networks. Source:(Meland et al., 2021).

4.3.9. Year 2020:

A vessel near Tynemouth: A maritime vessel anchored in the vicinity of Tynemouth, England, has been subject to a Ryuk ransomware attack, resulting in the encryption of its ship server and several client PCs. The IT service provider dispatched two specialists who determined that all data had been encrypted and irretrievably lost. A complete reinstallation was required to reinstate the systems. Source:(Meland et al., 2021).

Sodinokibi: Around the middle of the year 2020, the ransomware cyberattack known as Sodinokibi spreads throughout the administrative networks of three ships carrying the American flag. In addition to encrypting data, this malware also carries the risk of committing information theft (also known as "ransomtheft"). Source: (Meland et al., 2021).

MSC: MSC, a US-based gas pipeline operator and shipping company has experienced two separate malware incidents, with the latter forcing the closure of the shipowner's Geneva headquarters for five days. Sources: (Grinter, 2020; Maritime Executive, 2020c)

Shahid Rajaee port: The Iranian port of Shahid Rajaee, which is the newest of two major shipping ports in the city of Bandar Abbas on the Strait of Hormuz, suddenly stopped working for no apparent reason. All of the computers that control the flow of ships, trucks, and goods crashed at the same time. This caused huge delays on the rivers and roads that lead to the center. Israel is accused of breaching into the Iranian port of Shahid Rajaee, which stopped all shipping and goods for a long time. Sources: (Grinter, 2020; Warrick Joby and Nakashima, 2020).

Vard Group: Recently, the Norwegian shipbuilding company Vard Group AS encountered a ransomware attack at the Langsten shipyard. In light of the cyber-attack sustained by the servers at Langsten Shipyard, the company implemented all necessary measures for the resolution of the problem. It has been notified to numerous personnel that the interruptions could result in temporary unemployment because of suspended shipbuilding. Source: (Goud, 2020; Safety4sea, 2020b).

Carnival Corporation & plc: The cruise operator Carnival Corporation & plc has been subjected to two ransomware cyber-attacks between 2019 and 2020, likely resulting in the compromise of the personal data of customers and employees. Source: (Maritime Executive, 2020a).

Transport Malta: The Maltese transport authority experienced a debilitating malware cyber-attack resulting in the closure of its online systems for five days. Transport Malta implored its personnel to vigilantly observe their accounts for any potentially suspicious activity and to often modify their passwords, avoiding any passwords that can be easily ascertained or those that are identical for multiple accounts. Sources: (Agius, 2020; Azzopardi, 2020).

CMA CGM: The Ragnar Locker ransomware infects the computer systems of the French container transport business CMA CGM. A number of its branches in China were impacted, and the company was forced to temporarily disable a number of its internet services, including its scheduling system. Source: (Coble, 2020; Shen and Baker, 2020)

Red Funnel: British ferry company Red Funnel has been impacted by a malicious cyber-attack, resulting in a major disruption in its IT structures. Due to the unavailability of the reservation systems for some time, customers were necessitated to arrive earlier than the sailings to purchase tickets in person. Sources: (BBC News, 2020; Toogood, 2020).

Port of Kennewick: The Port of Kennewick in Washington State, USA has experienced a crippling ransomware cyber-attack on its IT systems. The hackers requested a ransom of two hundred thousand U.S. dollars, which was not received. The provenance of the attack is obscure; however, the authorities believe that it may have been initiated by a spurious email sent to a port staff member. The systems had to be reconstituted from offline backups, resulting in an extended period of unavailability. Source: (Maritime Executive, 2020d).

Hurtigruten: The Norwegian cruise operator Hurtigruten has experienced a detrimental ransomware cyber-attack, greatly compromising its IT structure. The company's public reports indicate that the probability that attackers had accessed larger amounts of guest data is minimal; however, Hurtigruten is not ruling out the possibility that some employee information might have been infiltrated. Sources: (Bøe and Jordheim, 2020; Maritime Executive, 2020b; Safety4sea, 2020a)

AIDA: The Doppel Paymer ransomware attack has affected the headquarters of the German travel provider AIDA, which is located in Rostock. Because of the severe IT problems caused by the assault, AIDA was forced to postpone several cruises. Source: (Walker, 2020).

4.3.10. Year 2021:

K-Line: In March 2021, the Japanese shipping company, 'K' Line, suffered a cyber-attack resulting in disruption to some of its enterprise systems. The company hypothesized that the deficit was a result of a malware infection initiated by its foreign affiliate. Due to the attack, it was necessary to suspend the operations of the enterprise systems and their external connections. Source: (Safety4sea, 2021b)

Cape Town and Durban: There has been a cyber-attack resulting in disruption to container operations at the ports of Cape Town and Durban in South Africa. A surge of cyber incidents has caused significant disruption to the operations of major ports in South Africa. The mining companies experienced significant losses due to the blackouts that occurred in Durban and Cape Town. Sources: (Le journal 2L'Afrique, 2021; Schenkelberg, 2021)

CMA CGM: The French shipping company CMA CGM has encountered its second cyber incident within less than one year. The company disclosed to its clientele that it has been subjected to another cyber assault. Approximately one ear prior, the French company experienced a ransomware cyber-attack of a similar nature. Sources: (Port Technology International, 2021; Safety4sea, 2021a)

4.3.11. Year 2022:

BlackCat: Several major oil terminals situated in a few of Western Europe's largest ports have been subject to a cyberattack. The Amsterdam-Rotterdam-Antwerp oil trading hub, which is a cross-border Dutch and Belgian entity, appears to be one of the prime casualties resulting from the attack, with corporate IT systems being adversely affected. The initial report by the German security services determined that the BlackCat ransomware was the malware utilized in the cyberattack in Germany. Sources: (RTE, 2022; Safety4sea, 2022b)

Port of Lisbon: In December of 2022, the Port of Lisbon underwent a cyber-attack, resulting in the shutdown of the port's website and internal computer networks. Cyber analysts additionally noted that the attack was perpetrated through a pervasive malware program labeled LockBit. The perpetrators disseminated statements via the 'darknet'. Sources: (Safety4sea, 2022a; The Portugal News/Lusa, 2022)

5. RESULTS

By the criteria outlined in the methodology section, an analysis of cyber-attacks targeting the maritime industry between 2010 and 2022 revealed that 30 out of a total of 40 attacks were related to the vulnerability of cyber security awareness. The disclosure indicates that among the 30 instances of attack, the vulnerability was exploited by hackers via social engineering in 12 cases through malware, 15 cases through ransomware, and 3 cases through phishing techniques which is depicted in Figure 2.

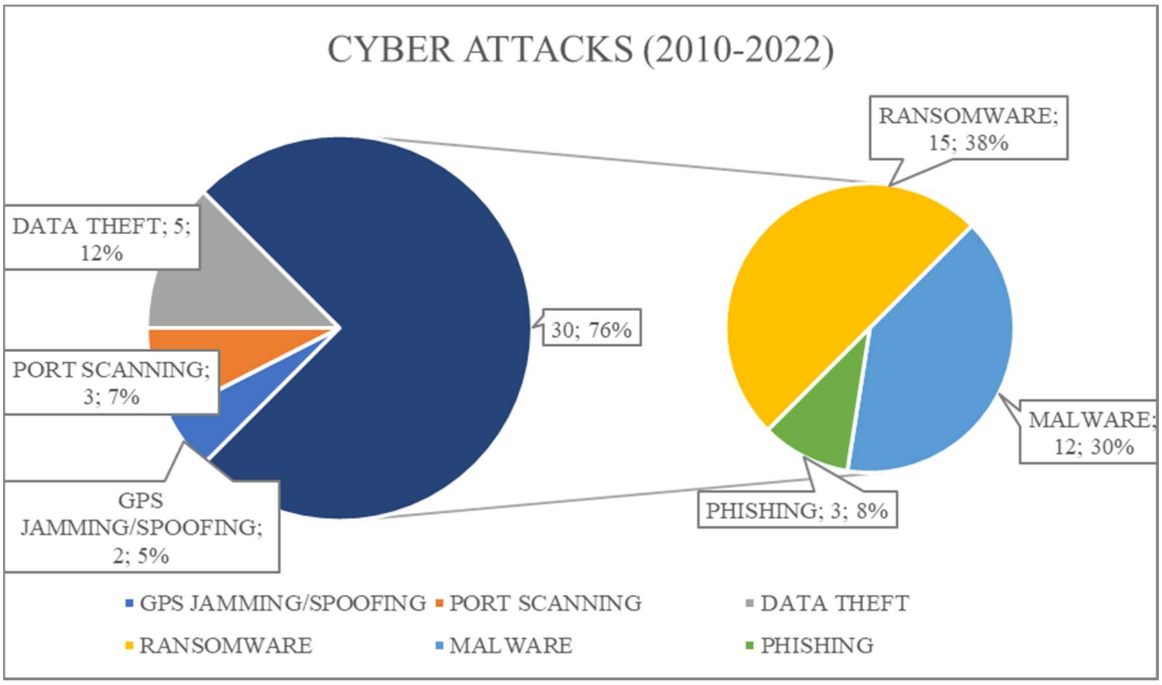


Fig. 2. Type-by-percentage analysis of cyber-attacks on the maritime industry between 2010 and 2022

Upon evaluating incidents about cybersecurity within the maritime industry, it has been observed that the absence of awareness and inadequate proficiency in cultivating secure conduct are significant contributors to the incidence of cybersecurity breaches. The observation of individuals who are engaged in cyber activities reveals that they lack awareness of the protective measures implemented to safeguard the system.

According to reports, there has been an increase in the occurrence of ransomware and other types of cyberattacks in 2020, with the maritime sector being among the recent targets of cybercriminals. Based on Naval Dome, a cybersecurity expert, there was a rise of 400% in attempted cyberattacks on the maritime sector between February 2020 and December 2020. This increase in attacks coincides with the industry's heightened reliance on technology and remote work arrangements, which were adopted as a response to the COVID-19 pandemic. The rise in phishing attempts, malware, and ransomware attacks can be linked to the alterations in operations and procedures resulting from travel restrictions and operational obstacles experienced during the pandemic. (Hellenic Shipping News Worldwide, 2020)

Another study that reveals the cyber security vulnerabilities of employees is Bolat and Kayişoğlu (2019) *"Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector"*. As an output of their study:

- Education plays a significant role in enhancing cybersecurity awareness among maritime employees, positively impacting their behavior concerning cybersecurity.
- Personal experiences with cybersecurity incidents have a noteworthy influence on employee cybersecurity awareness and their subsequent behavior in this domain.
- Maritime cybersecurity awareness has a substantial impact on promoting secure user behavior among employees.

Furthermore, the study reveals that rules and policies related to information sharing do not significantly affect cybersecurity awareness or the development of secure employee behavior. (Bolat and Kayişoğlu, 2019)

Thus, it can be concluded that the maritime transportation industry poses a significant level of risk about cybersecurity, while simultaneously exhibiting a low level of awareness in this domain. The aforementioned assertion was corroborated by the European Network and Information Security Agency, which identified seven significant inadequacies of cybersecurity in the maritime sector, as outlined in reference (ENISA, 2011a).

- "Low awareness and focus.
- Complex structure of Maritime systems.
- Absence of holistic management approach in national and international contexts in the maritime field.
- Inadequacies related to the security of cyberspace in maritime regulations.
- No holistic understanding of cybersecurity.
- Lack of economic incentives and initiatives for work to increase cybersecurity in the maritime sector.
- Lack of incentives to motivate work."

6. CONCLUSION

Technological developments and Industry 4.0 have made rapid and effective decision-making processes and cost-effective operations possible in the maritime sector. Blockchain, smart ports, autonomous ships, IoT-based real-time monitoring, digital twins, and similar technologies are innovations that the cyber world has brought to the maritime industry. Nevertheless, the technological advancements in the maritime industry have certain unfavorable implications. The emergence of innovations in technology has resulted in susceptibility to cyber-attacks in the maritime industry, thereby creating opportunities for both criminal actors and commercial stakeholders.

Regardless of the different subfields, the common finding of all studies related to cybersecurity is that employees' cybersecurity awareness levels are very low, and significant and selfless efforts are required to improve the situation. Moreover, it is known that the ongoing malicious activities in the sector do not represent the true amount of publicly reported incidents, and there is a significant difference between reported incidents and actual rates. This study highlights the role of human cybersecurity awareness in successful cyber-attacks in the maritime sector. When analyzing attacks carried out since 2010, it was found that 76% were carried out through social engineering methods such as phishing, malware, and ransomware. The individuals targeting stakeholders in the maritime industry are cognizant of the fact that employees within the industry lack adequate cybersecurity awareness and a comprehensive grasp of cybersecurity principles. While certain initiatives like the *"Manual on the International Law Applicable to Cyber Warfare"* also known as the *"Tallinn Manual"*[2] have emerged from an expert-driven process to create a non-

[2] The Tallinn Manual, initially named the Tallinn Manual on the International Law Applicable to Cyber Warfare, serves as an academic exploration into the application of international law in the context of cyber conflicts and warfare. Produced between 2009 and 2012, the manual was authored by an international assembly of roughly twenty experts at the request of the NATO Cooperative Cyber Defence Centre of Excellence located in Tallinn. (Schmitt, 2017)

binding document that applies existing laws to cyber warfare, the intricate nature of these systems makes it challenging to establish a permanent and universally applicable solution. This thesis is supported by the fact that three out of every four cyber-attacks managed within the scope of the criteria in the methodology section are due to a lack of cyber security awareness.

To prevent situational awareness vulnerabilities in humans, the role of human behavior in cybersecurity structures should be taken more into account. Within the scope of Industry 5.0, which offers a new perspective, especially towards the use of technology for the benefit of society and aims to eliminate the disadvantages created by Industry 4.0, it is considered necessary to move the human factor from an operational position to a supervision and decision-making authority position, to minimize human-caused cybersecurity vulnerabilities in execution.

As highlighted in this study, the success of cyberattacks on the maritime industry is directly proportional to the vulnerability in employees' cybersecurity awareness. Therefore, future studies should concentrate on measures to eliminate this vulnerability, aiming for more rapid, secure, and efficient utilization of the benefits brought about by technology. Prioritizing awareness-enhancing training over physical measures in these efforts and presenting alternatives for achieving this goal will lead to productive outcomes based on the results obtained in this study.

REFERENCES

Agius, M. (2020). *TM mum on whether cyber-attack affected ship, air registries - Newsbook.* https://newsbook.com.mt/en/tm-mum-on-whether-cyber-attack-affected-ship-air-registries/

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, *45*, 547–554. https://doi.org/10.1016/j.trpro.2020.03.058

Algarni, A., Xu, Y., Taizan Chan, & Yu-Chu Tian. (2013). Social engineering in social networking sites: Affect-based model. *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, 508–515. https://doi.org/10.1109/ICITST.2013.6750253

Athens Group Services. (2019). *Cybersecurity – There Is No Silver Bullet.* https://athensgroupservices.com/cybersecurity-there-is-no-silver-bullet/

Azzopardi, K. (2020). *Investigation into Transport Malta cyber-attack has not yet determined whether hack led to data leakage.* https://www.maltatoday.com.mt/news/national/105593/watch_transport_malta_cyber_attack_investigation_has_not_yet_determined_whether_data_was_stolen#.ZBW3OhTP25c

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *Cornell University, Computer Science, Cryptography and Security.* https://doi.org/https://doi.org/10.48550/arXiv.1901.02672

BBC News. (2020). *Red Funnel ferry firm's IT system hit by "malicious attack."* https://www.bbc.com/news/uk-england-hampshire-54368110

Bolat, P. & Kayişoğlu, G. (2019). Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector. Journal of ETA Maritime Science, 7(4), 344-360.

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*, *13*(1), 22. https://doi.org/10.3390/info13010022

Bøe, E., & Jordheim, H. (2020). *Police investigate the computer attack against Hurtigruten – E24.* https://e24.no/hav-og-sjoemat/i/7KPeEK/politiet-etterforsker-dataangrepet-mot-hurtigruten

Borazjani, P. N. (2017). *Security Issues in Cloud Computing* (pp. 800–811). https://doi.org/10.1007/978-3-319-57186-7_58

Buurma, C., & Sebenius, A. (2020). *Ransomware Shuts U.S. Natural Gas Compressor Facility for Two Days.* https://www.carriermanagement.com/news/2020/02/20/203485.htm

Čekerevac, Z., Dvorak, Z., Prigoda, L., & Čekerevac, P. (2017). Man-In-The-Middle Attacks and Internet Of Things. *FBIM Transactions*, *5*(2). https://doi.org/10.12709/fbim.05.05.02.03

Cimpanu, C. (2018a). *Ransomware Infection Cripples Shipping Giant COSCO's American Network.* https://www.bleepingcomputer.com/news/security/ransomware-infection-cripples-shipping-giant-coscos-american-network/

Cimpanu, C. (2018b). *Ransomware Infection Cripples Shipping Giant COSCO's American Network.* https://www.bleepingcomputer.com/news/security/ransomware-infection-cripples-shipping-giant-coscos-american-network/

Cimpanu, C. (2019). *US Coast Guard discloses Ryuk ransomware infection at maritime facility | ZDNET*. https://www.zdnet.com/article/us-coast-guard-discloses-ryuk-ransomware-infection-at-maritime-facility/

CISA-US. (2020). *Avoiding Social Engineering and Phishing Attacks | CISA*. https://www.cisa.gov/uscert/ncas/tips/ST04-014

Clark, J. (2018). Cybercrime in the shipping industry. *A Presentation by Shipping Hill Dickinson LLP*.

Coble, S. (2020). *Ransomware Attack on Shipping Giant*. https://www.infosecurity-magazine.com/news/ransomware-attack-on-shipping-giant.

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Computers in Industry, 114, 103165. https://doi.org/10.1016/j.compind.2019.103165

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *49*(3), 229–233. https://doi.org/10.1177/154193120504900304

Dragos. (2020). *Assessment of Ransomware Event at U.S. Pipeline Operator*. https://www.dragos.com/blog/industry-news/assessment-of-ransomware-event-at-u-s-pipeline-operator/

ENISA. (2011a). *Analysıs of Cybersecurity Aspects in The Marıtıme Sector.*

ENISA. (2011b). *Cyber Security Aspects in the Maritime Sector*. https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

Fitton, M. O., Prince, D., & Lacy, M. (2015). *The Future of Maritime Cyber Security*. https://eprints.lancs.ac.uk/id/eprint/72696/

Futurenautics Maritime-KVH and Intelsat. (2018). *Crew Connectivity 2018 Survey Report Maritime*. http://www.navarino.co.uk/wp-content/uploads/2018/04/Crew_Connectivity_2018_Survey_Report.pdf

Goud, N. (2019). *Cyber Attack on James Fisher and Sons - Cybersecurity Insiders*. https://www.cybersecurity-insiders.com/cyber-attack-on-james-fisher-and-sons/

Goud, N. (2020). *Ransomware attack on Norwegian Ship yard results in job loss to many - Cybersecurity Insiders*. https://www.cybersecurity-insiders.com/ransomware-attack-on-norwegian-ship-yard-results-in-job-loss-to-many/

Grinter, M. (2020). *Maritime cyber-attacks up 900% in three years - Hong Kong Maritime Hub*. http://www.hongkongmaritimehub.com/maritime-cyber-attacks-up-900-in-three-years/

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629–3654. https://doi.org/10.1007/s00521-016-2275-y

Hareide, O. S., Jøsok, Ø., Lund, M. S., Ostnes, R., & Helkala, K. (2018). Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *Journal of Navigation*, *71*(5), 1025–1039. https://doi.org/10.1017/S0373463318000164

Hellenic Shipping News Worldwide. (2020). *Greater Cyber Security Needed For Coronavirus And Economic Crises*. https://www.hellenicshippingnews.com/greater-cyber-security-needed-for-coronavirus-and-economic-crises/

Hindy, H., Tachtatzis, C., Atkinson, R., Bayne, E., & Bellekens, X. (2021). Developing a Siamese Network for Intrusion Detection Systems. *Proceedings of the 1st Workshop on Machine Learning and Systems*, 120–126. https://doi.org/10.1145/3437984.3458842

IMO. (2017). *Guidelines on Maritime Cyber Risk Management.* https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf

Interpol. (2020). *Cyber Crime: COVID-19 Impact*. https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf?inLanguage=eng-GB

Jensen, L. (2015). Challenges in Maritime Cyber-Resilience. *Technology Innovation Management Review*, *5*(4), 35–39. https://doi.org/10.22215/timreview/889

Kapalidis, P. (2020). Cybersecurity at Sea. In L. Otto (Ed.), *Global Challenges in Maritime Security. Advanced Sciences and Technologies for Security Applications.* (pp. 127–143). https://doi.org/10.1007/978-3-030-34630-0_8

Kessler, G. C., & Uk, A. (n.d.). *Cybersecurity in the Maritime Domain Cybersecurity in the Maritime Domain CORE View metadata, citation and similar papers at core*. Retrieved March 21, 2023, from https://commons.erau.edu/publication/1318

Kim, J., & Saul, J. (2016). *South Korea Revives GPS Backup Project After Blaming North for Jamming*. https://gcaptain.com/south-korea-revives-gps-backup-project-after-blaming-north-for-jamming/

Kokar, M. M., & Endsley, M. R. (2012). Situation Awareness and Cognitive Modeling. *IEEE Intelligent Systems*, *27*(3), 91–96. https://doi.org/10.1109/MIS.2012.61

Lam, J. S. L., & Bai, X. (2016). A quality function deployment approach to improve maritime supply chain resilience. *Transportation Research Part E: Logistics and Transportation Review*, *92*, 16–27. https://doi.org/10.1016/j.tre.2016.01.012

Larsen, M. H., & Lund, M. S. (2021). Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review. *IEEE Access*, *9*, 144895–144905. https://doi.org/10.1109/ACCESS.2021.3122433

Le journal 2L'Afrique. (2021). *Cyber attacks cripple South African ports*. https://lejournaldelafrique.com/en/cyber-attacks-paralyze-South-African-ports/

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Lemos, R. (2019). *Coast Guard Warns Shipping Firms of Maritime Cyberattacks*. https://www.darkreading.com/vulnerabilities-threats/coast-guard-warns-shipping-firms-of-maritime-cyberattacks

Linton, A. (2016). *Port Authority Role in Cyber-Security -LinkedIn*. https://www.linkedin.com/pulse/port-authority-role-cyber-security-art-linton/

Lubold, G., & Volz, D. (2018). *Chinese Hackers Breach U.S. Navy Contractors - WSJ*. https://www.wsj.com/articles/u-s-navy-is-struggling-to-fend-off-chinese-hackers-officials-say-11544783401

Mahoney, S., Roth, E., Steinke, K., Pfautz, J., Wu, C., & Farry, M. (2010). Cognitive Task Analysis for Cyber Situational Awareness. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *54*(4), 279–283. https://doi.org/10.1177/154193121005400403

Mallik, A., Ahsan, A., Shahadat, M. Md. Z., & Tsou, J.-C. (2019). Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science*, 77–92. https://doi.org/10.5267/j.ijdns.2019.1.001

Maritime Executive. (2020a). *Carnival Corporation Reports Ransomware Attack Accessed Data*. https://www.maritime-executive.com/article/carnival-corporation-reports-ransomware-attack-accessed-data

Maritime Executive. (2020b). *Hurtigruten Reports Passenger Data Exposed in Cyberattack*. https://www.maritime-executive.com/article/hurtigruten-reports-passenger-data-exposed-in-cyberattack

Maritime Executive. (2020c). *Naval Dome: Cyberattacks on OT Systems on the Rise*. https://www.maritime-executive.com/article/naval-dome-cyberattacks-on-ot-systems-on-the-rise

Maritime Executive. (2020d). *Ransomware Cripples IT Systems of Inland Port in Washington State*. https://www.maritime-executive.com/article/ransomware-attack-cripples-systems-of-inland-port-in-washington-state

McNeese, M., Cooke, N. J., D'Amico, A., Endsley, M. R., Gonzalez, C., Roth, E., & Salas, E. (2012). Perspectives on the Role of Cognition in Cyber Security. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *56*(1), 268–271. https://doi.org/10.1177/1071181312561063

Mcquade, M. (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Meland, P. Há., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A Retrospective Analysis of Maritime Cyber Security Incidents. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, *15*(3), 519–530. https://doi.org/10.12716/1001.15.03.04

Mraković, I., & Vojinović, R. (2019a). Maritime Cyber Security Analysis – How to Reduce Threats? *Transactions on Maritime Science*, *8*(1), 132–139. https://doi.org/10.7225/toms.v08.n01.013

Mraković, I., & Vojinović, R. (2019b). Maritime Cyber Security Analysis – How to Reduce Threats? *Transactions on Maritime Science*, *8*(1), 132–139. https://doi.org/10.7225/toms.v08.n01.013

Mraković, I., & Vojinović, R. (2019c). Maritime Cyber Security Analysis – How to Reduce Threats? *Transactions on Maritime Science*, *8*(1), 132–139. https://doi.org/10.7225/toms.v08.n01.013

Nguyen, L. (2018, February). *e-paper: Collaboration in the Shipping Industry: Innovation and Technology*. KNect365. https://informaconnect.com/epaper-collaboration-in-the-shipping-industry-innovation-and-technology/

NSI, N. S. I. (2017). *A Brief User's Guide to Getting the Most from Your Employee Security Connection Subscription*. https://www.nsi.org/pdf/ESC_User's_Guide.pdf

Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems*, *37*. https://doi.org/10.17705/1CAIS.03743

Parizo, E. (2019). *Maersk CISO Says NotPeyta Devastated Several Unnamed US firms*. https://www.darkreading.com/omdia/maersk-ciso-says-notpeyta-devastated-several-unnamed-us-firms

Perez, G. F. (2019). *Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry* [Nova Southeastern University]. https://nsuworks.nova.edu/gscis_etd

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

Port Technology International. (2021). *CMA CGM faces cyber attack leading to data leak - Port Technology International*. https://www.porttechnology.org/news/cma-cgm-faces-cyber-attack-leading-to-data-leak/

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber Physical Systems Security for Maritime Assets. *Journal of Marine Science and Engineering*, *9*(12), 1384. https://doi.org/10.3390/jmse9121384

Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-Risk Management*. Springer International Publishing. https://doi.org/10.1007/978-3-319-23570-7

Reuters. (2012). *Saudi Arabia says cyber attack aimed to disrupt oil, gas flow | Reuters*. https://www.reuters.com/article/saudi-attack/saudi-arabia-says-cyber-attack-aimed-to-disrupt-oil-gas-flow-idUSL5E8N91UE20121209

RTE. (2022). *European oil port terminals hit by cyberattack*. https://www.rte.ie/news/world/2022/0203/1277569-oil-terminal-cyberattack/

S. de Vleeschhouwer. (2017). *Safety of data. The risks of cyber security in the maritime sector*. https://maritimetechnology.nl/media/NMT_Safety-of-data-The-risks-of-cyber-security-in-the-maritime-sector.pdf

Safety4sea. (2018). *2018 Highlights: Major cyber-attacks reported in maritime industry*. https://safety4sea.com/cm-2018-highlights-major-cyber-attacks-reported-in-maritime-industry/

Safety4sea. (2020a). *Hurtigruten hit by cyber-attack*. https://safety4sea.com/hurtigruten-hit-by-cyber-attack/

Safety4sea. (2020b). *Vard shipbuilder experiences ransomware attack - SAFETY4SEA*. https://safety4sea.com/vard-shipbuilder-experiences-ransomware-attack/

Safety4sea. (2021a). *CMA CGM face to face with another cyber-attack - SAFETY4SEA*. https://safety4sea.com/cma-cgm-face-to-face-with-another-cyber-attack/

Safety4sea. (2021b). *K Line issues apology after yet another cyber-attack*. https://safety4sea.com/k-line-issues-apology-after-yet-another-cyber-attack/

Safety4sea. (2022a). *Cyber attack hits Port of Lisbon*. https://safety4sea.com/cyber-attack-hits-port-of-lisbon/

Safety4sea. (2022b). *Cyber attacks hit European oil terminals - SAFETY4SEA*. https://safety4sea.com/cyber-attacks-hit-european-oil-terminals/

Schenkelberg, B. (2021). *S. Africa Cyber-Attack, Durban & Richards Bay Terminals - X-Industry - Red Sky Alliance*. https://redskyalliance.org/xindustry/s-africa-cyber-attack-durban-richards-bay-terminals

Schmitt, M. (2017). Introduction. In Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (pp. 1-8). Cambridge: Cambridge University Press. doi:10.1017/9781316822524.006

Secureworks. (2018). *Gold Galleon: How a Nigerian Cyber Crew Plunders the Shipping Industry*. https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry

Shauk, Z. (2013, April 28). *Malware on the offshore rig: Danger lurks where the chips fail*. https://www.houstonchronicle.com/business/energy/article/Malware-on-the-offshore-rig-Danger-lurks-where-4470723.php

Shen, C., & Baker, J. (2020). *CMA CGM confirms ransomware attack*. https://lloydslist.maritimeintelligence.informa.com/LL1134044/CMA-CGM-confirms-ransomware-attack

Tam, K., & Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, Port*18*(1), 129–163. https://doi.org/10.1007/s13437-019-00162-2

The Maritime Executive. (2018). *Saipem's Servers Hit by Cyberattack*. https://maritime-executive.com/article/saipem-s-servers-hit-by-cyberattack

The Norwegian National Security Authority (NSM). (2020). *RISIKO 2020*. https://www.digi.no/filer/NSM_Risiko_2020_a_pen.pdf

The Portugal News/Lusa. (2022). *Cyberattack at Lisbon port - The Portugal News*. https://www.theportugalnews.com/news/2022-12-26/cyberattack-at-lisbon-port/73281

Toogood, D. (2020). *Red Funnel Suffers "Malicious Attack" on IT Systems Causing Major Disruption*. https://www.islandecho.co.uk/red-funnel-suffers-malicious-attack-on-it-systems-causing-major-disruption/

Torbati, Y., & Saul, J. (2012, October). *Iran's top cargo shipping line says sanctions damage mounting | Reuters*. https://www.reuters.com/article/us-iran-sanctions-shipping-idUSBRE89L10X20121022

Volz, D. (2019). *Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets - WSJ*. https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800

Walker, J. (2020). *AIDA Cruise Ships Under Cyber Attack - Are Costa Ships Also Affected? | Cruise Law News*.https://www.cruiselawnews.com/2020/12/articles/cyber-attacks/aida-cruise-ships-under-cyber-attack-are-costa-ships-also-affected/

Walker, J., & Spencer, J. (n.d.). *Cyber Marine: Risks & Loss Scenarios*. International Marine Claims Conference. Retrieved March 8, 2023, from http://www.marineclaimsconference.com/imcc-docs/docs/Cyber%20workshop.pdf

Warrick Joby, & Nakashima, E. (2020). *Officials: Israel linked to a disruptive cyberattack on Iranian port facility - The Washington Post*. https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering - EASE '14*, 1–10. https://doi.org/10.1145/2601248.2601268

Mersin University Journal of Maritime Faculty

Mersin University Journal of Maritime Faculty (MEUJMAF)
Vol. 5, Issue 2, pp. 37-44, December 2023
e-ISSN 2687-6612, Türkiye
DOI: 10.47512/meujmaf.1373811
Research Article

ANALYSIS OF NAVTEX MESSAGES PUBLISHED FOR THE MEDITERRANEAN REGION IN TERMS OF SAFE NAVIGATION OF SHIPS

Ali Ekrem Akyol[1], Tuba Keçeci *[2]

[1] Istanbul Technical University, Faculty of Maritime, Department of Maritime Transportation Management Engineering,
Istanbul, Türkiye
ORCID ID 0009 – 0006– 4640– 6999
akyola18@itu.edu.tr

[2] Istanbul Technical University, Faculty of Maritime, Department of Maritime Transportation Management Engineering,
Istanbul, Türkiye
ORCID ID 0000-0001-6259-3858
kececit@itu.edu.tr

* Corresponding Author

Received: 10/10/2023 Accepted: 23/12/2023

ABSTRACT

Navigational Telex (NAVTEX) messages have a significant impact on the navigational safety of ships. NAVTEX plays an important role in decreasing the chances of near-misses, groundings, and collisions in the sea by disseminating safety-related information. In this study, it was aimed to present that navigational risk trend in a region could be revealed by analyzing NAVTEX messages. The analysis of NAVTEX messages as a data set will constitute a good data source for ship managers, researchers and seafarers who are navigating on the seas. Since there is no current research on NAVTEX messages in terms of navigational safety focused on Mediterranean Sea in the literature, this study aimed to fill this gap. The NAVTEX messages that pertain to the Mediterranean region were examined in the notice to mariners bulletin published by the Turkish Naval Forces Office of Navigation, Hydrography and Oceanography between 2019 and 2022. The examination was limited to messages broadcast from Antalya station. The study employed the document analysis method. The distribution of the number of messages by year, the annual distribution of messages by topic, and the annual distribution of messages by type were determined as the main research questions. It has been observed that studying the trends of NAVTEX messages can provide significant data about the region. It has been evaluated that this approach will contribute to the decision-making mechanisms of ship managers, particularly seafarers, and can serve as a source of information for rule makers. This study was produced by developing the undergraduate thesis titled "Review of NAVTEX Messages for the Mediterranean Sea Published in Notice to Mariners", which was completed successfully in June 2023.

Keywords: *Maritime Transportation, Ship Management, NAVTEX, Safety, Mediterranean Sea*

1. INTRODUCTION

To ensure safe navigation, ships must have information about the region they are in. Obtaining up-to-date information about weather condition, water depth, and currents, as well as the presence of an element that could adversely affect navigation safety, is crucial. Emergency situations can be managed promptly by being instantly informed of important conditions in the navigation area and the negativities encountered by other ships. It contributes to the safety and security of ship crew and passengers, which in turn increases navigational safety in general.

Safety at sea is ensured through the publication of international standards and regulations. The International Maritime Organization (IMO) is the source of these publications. The aim of these rules is to improve the efficiency of the systems and equipment employed on ships. Communication between shore and ship stations is provided by the Global Maritime Distress Safety System (GMDSS), which is one of these systems. Rapid communication in emergencies and routine communication are possible with the use of GMDSS system, which consists of a series of equipment. The NAVTEX system, which is shortened to Navigational Telex, is a component of the GMDSS system. Emergency messages may also be included in NAVTEX messages that convey important navigational information. NAVTEX messages contain a variety of warnings, including navigation aid status, weather forecast, search and rescue (SAR) activities, environmental information, underwater work, and warnings about fishing vessels. The navigational safety of the ship could be affected by these messages and it may be necessary for the ship to change its route. Ship crew are now able to take early precautions against possible dangers thanks to the NAVTEX messages. Kaptan and Ugurlu (2022) studied how electronic navigation devices contribute to marine accidents. A total of 153 accidents that were published by 9 different accident research institutions were reviewed in the study. It was stated that the error in selecting the station of the NAVTEX device caused a ship collision. Similarly, according to the safety investigation report published by Transport Malta's Marine Safety Investigation Unit (MSIU), NAVTEX operating error was stated among the probable causes in the grounding incident of the oil tanker Hephaestus (Safety4sea, 2023). Therefore, the analysis of NAVTEX messages is important in the context of maritime safety.

This study examined NAVTEX messages that were published in one of the seas surrounding Turkey, with the idea that examining the content of NAVTEX messages within a specific region may provide insight into navigational safety in that region. It is aimed to reveal some information about the topics on which messages are published most, what the type of messages are and the annual change in the number of messages. The results will assist in making suggestions to enhance safety based on the information obtained. The Mediterranean Sea was selected as the area of study. The Mediterranean Sea has always been the location of many activities, such as maritime trade and fishing. The Black Sea countries have their sea exit route through the Mediterranean, which opens to the Suez Canal. Due to the constant use of commercial ships, there is a high volume of maritime traffic in the area. The geographical features and geopolitical position make it one of the most important sea areas in the world. Furthermore, the Eastern Mediterranean's dynamism has been enhanced by research and work on energy resources. It is crucial for ships sailing in the region to have knowledge about the region to ensure their safety. (Kedikli & Çalağan, 2017).

This study examined the NAVTEX warnings in the notice to mariners published by the Turkish Naval Forces Office of Navigation Hydrography and Oceanography, that pertain to the Mediterranean region. Only the messages broadcast from Antalya station were analyzed. Other countries' announcements regarding this region were excluded. The data for the years 2019-2022 was analyzed. The data was categorized under the standard message type classes of NAVTEX. By contributing to the safe operation of ships, it aims to increase safety in the maritime sector by providing useful information to ships sailing in the Mediterranean. In this study, it was aimed to present that navigational risk trend in the region could be revealed by analyzing NAVTEX messages. It was assessed that using big data analysis approach to review NAVTEX messages would increase navigational safety.

This is the first study that examines the NAVTEX warnings for the Mediterranean Sea included in notice to mariners published by the Turkish Naval Forces Office of Navigation Hydrography and Oceanography in terms of navigational safety. It will be a great resource for literature. The significance of NAVTEX messages in safeguarding maritime operations and preventing accidents at sea cannot be underestimated. Thus, this study is significant due to its potential to inspire future research. The next section of the study contained information about NAVTEX and references to studies in the literature. Section 3 outlines the methodology. This section provides an explanation of data classification, research questions, and data analysis method. In Section 4, the study's findings are presented. The study results' and advantages are discussed in Section 5.

2. NAVTEX

Maritime safety information (MSI) encompasses numerous navigational and meteorological warnings, as well as urgent safety-related messages that need to be distributed to ships in different areas of navigation (Zanic Mikulicic, 2018). Narrow Band Direct Printing Telegraphy also sends MSIs, which are received by the NAVTEX receiver. NAVTEX uses 518 kHz frequency on which coast stations transmit information and the range of about 250 to 400 nautical miles is intended to prevent mutual interference and transmissions (Korcz, 2011). On a time-sharing basis, the transmission is transmitted in English. The message types that the NAVTEX device receives are explained in IMO MSC.1/Circ.1403 as illustrated in Table 1.

Table 1. Characters and types of NAVTEX messages (IMO MSC.1/Circ.1403)

Identification character	Type
A	Navigational warnings
B	Meteorological warnings
C	Ice reports
D	Search and rescue information, acts of piracy warnings, tsunamis and other natural phenomena
E	Meteorological forecasts
F	Pilot and VTS service messages
G	AIS service messages (non-navigational aid)
H	LORAN messages
I	Currently not used
J	GNSS messages regarding PRN status
K	Other electronic navigational aid system messages
L	Other navigational warnings
M, N, O, P, Q, R, S, T, U	Currently not used
V, W, X, Y	Special services allocation by the IMO NAVTEX coordinating Panel
Z	No message

NAVTEX and maritime safety are covered in various studies in the literature. An application was developed by Lee and Lee (2013) that displays NAVTEX messages on Android mobile devices. Korcz (2016) analyzed the operational and technical capabilities of marine communication systems to guarantee maritime safety and security. The author concluded that the combination of NAVTEX and the SafetyNET service via the Inmarsat EGC service is a highly reliable method of disseminating warnings. The study pointed out that implementing new technology is the only way to achieve navigational safety and security. Yao et al. (2017) proposed a design for the exciter of the weather fax chart and NAVTEX message. Liu et al. (2018) investigated a classification system that uses the Bayes Theorem for MSIs. from 2011 to 2016, thousands of NAVTEX messages were collected by the authors and they compared naive Bayes classifiers with different event models. They concluded that the method proposed to use Naive Bayes theory to classify MSI is feasible and can result in a good classification effect. Borisova et. al. (2020) examined the improvement of the telecommunication support of navigational safety systems in the Arctic. One of the conclusions that the authors reached is that the deployment of NAVTEX automated systems and high-frequency coastal equipment should be included in the construction of marine rescue coordination centers.

It is observed in the literature that the studies on NAVTEX messages specific to the Mediterranean region (Oral, 2021; Şen and Açıkgöz, 2022; Ogurlu and Ozsaglam, 2022) are generally linked to politics. As there is no current research on NAVTEX messages in terms of navigational safety focused on Mediterranean Sea in the literature this study will be the first to be published on this subject.

3. METHOD

The research was conducted using a document analysis method. The process of document analysis involves examining and evaluating materials in electronic or printed media (Bowen, 2009). The document analysis process is depicted in Kiral (2020)'s study as shown in Figure 1.

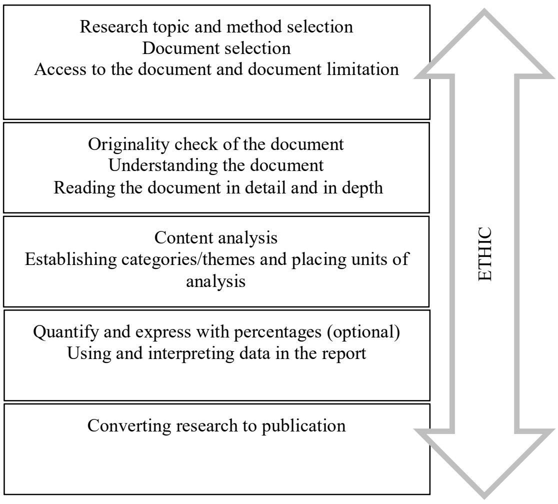

Research topic and method selection
Document selection
Access to the document and document limitation
Originality check of the document
Understanding the document
Reading the document in detail and in depth
Content analysis
Establishing categories/themes and placing units of analysis
Quantify and express with percentages (optional)
Using and interpreting data in the report
Converting research to publication
ETHIC

Fig. 1. Document analysis process Kıral (2020)

The process begins with choosing the subject and accessing the document, and continues with a detailed examination of the document, as shown in Figure 1. Afterward, the data obtained through content analysis is analyzed and published. Ethics appears to be the fundamental element of this process.

NAVTEX messages published in the Mediterranean Sea were examined within the scope of the research. The research focused solely on Türkiye's published messages, while other countries' announcements regarding this region were excluded. The information under the heading "NAVTEX message" in the Notices to Mariners Bulletin published regularly on the website of the Turkish Naval Forces Office of Navigation, Hydrography and Oceanography was used. Weekly publication is the norm for this bulletin. The validity and reliability of the research is enhanced by the use of an institutional report. According to Baltacı (2019), the degree to which the researcher solves the problem objectively is known as validity, and reliability is related to the repeatability of the results. It is considered that this study is valid and reliable because the information in the notice to mariners is presented in an understandable, clear and organized manner and the data used within the scope of the research is not modified.

Detailed information about the data analysis stages is presented under the headings of Section 3.1 Data Classification, Section 3.2 Research Questions, and Section 3.3 Data Analysis.

3.1. Data Classification

The following categories were determined to examine the data through content analysis.

- Notice number (week/year)
- Message number
- Serial number
- Continuing/Discontinued identification
- Station code
- Message type
- Message topic
- Message content
- Position information

Codes are used to categorize some of these categories within themselves. The explanations under the category headings below provide detailed information about classification. An Excel file was used to process the data for the years 2019-2022.

3.1.1. Notice number

The notice number provides us with information about the week and year in which the message was published. The messages for the first week of the year are numbered 01. The messages for the final week of the year are numbered 52. The week number is followed by the year information.

3.1.2. Message number

Each message published by the Turkish Naval Forces Office of Navigation, Hydrography and Oceanography has a distinct message number assigned to it. The processing of messages is prevented from any confusion by this method. The archiving process is also made easier by it.

3.1.3. Serial number

The serial number of a message can be used to determine the year the message was published by the Turkish Naval Forces Office of Navigation, Hydrography and Oceanography.

3.1.4. Continuing/Discontinued Series Identification

NAVTEX messages are divided into two categories: continuing and discontinued. A continuing series is defined as messages that have been published and are valid at later dates. Discontinued series are messages that are published once and do not remain valid at later dates. The analysis phase in this study was organized by assigning codes "1" to continuing series and "2" to discontinued series during the data processing phase.

3.1.5. Station Code

NAVTEX messages are broadcasted by Coastal Radio Stations (CRS). Stations in Istanbul, Antalya, Samsun, and Izmir in Türkiye produce these broadcasts.

This study will only examine NAVTEX messages that were published for the Mediterranean Sea. The messages broadcast from Antalya station were analyzed for this reason. Istanbul station was coded as "1", Samsun station was coded as "2, Izmir station was coded as "3, and Antalya station was coded as "4" during the data extraction process.

3.1.6. Message type

To define the message type, 6 separate classes have been determined in accordance with NAVTEX standards. The data was recorded by assigning a code to each class.

- The code for navigational warnings (A) is '1'. Announcements about significant malfunctions in navigation aids, marine accidents, fires, suspicious objects, underwater work, wrecks, and shallows are included under this message type.
- The code for meteorological warnings (B) is '2'. The purpose of these warnings is to provide information about meteorological events.
- The code for ice warnings (C) is '3.' There are no warnings of this nature in the region. To avoid disrupting the NAVTEX message category order, this category was also numbered and added to the analysis process.
- The code for Search and Rescue Activities and Piracy (D) is '4.' The purpose of this broadcast is to inform ships about search and rescue activities. This class also includes announcements to alert other ships in case of a piracy activity.
- The code for the weather forecast (E) is '5'. This class includes weather forecast reports.
- The code for pilotage (F) is '6'. This class contains information about pilotage messages made by ports.

3.1.7. Message topic

According to the content of the message, to better comprehend the topic on which it was published and present it in numerical results, 7 message topic classes were established. Below is a list of the classes and their assigned codes.

Aids to navigation messages are encoded with '1'.

The code for messages about shipwrecks and floating objects is '2'.

Messages that pertain to underwater work and scientific research are encoded with '3'.

Military activities and drills are coded with '4.'

Messages about piracy are coded with '5'.

The code for messages about mines is '6'.

The code for other messages is '0'.

3.1.8. Message content

The purpose of this category is to examine the content of NAVTEX messages. The codes under the message topic heading were assigned after reading the contents.

3.1.9. Position information

The purpose of creating this category was to comprehend the latitude and longitude of the warning subject to the message.

3.2. Research questions

The research's objective was to uncover answers to the following questions.

Question 1: What is the distribution of the number of messages by years?

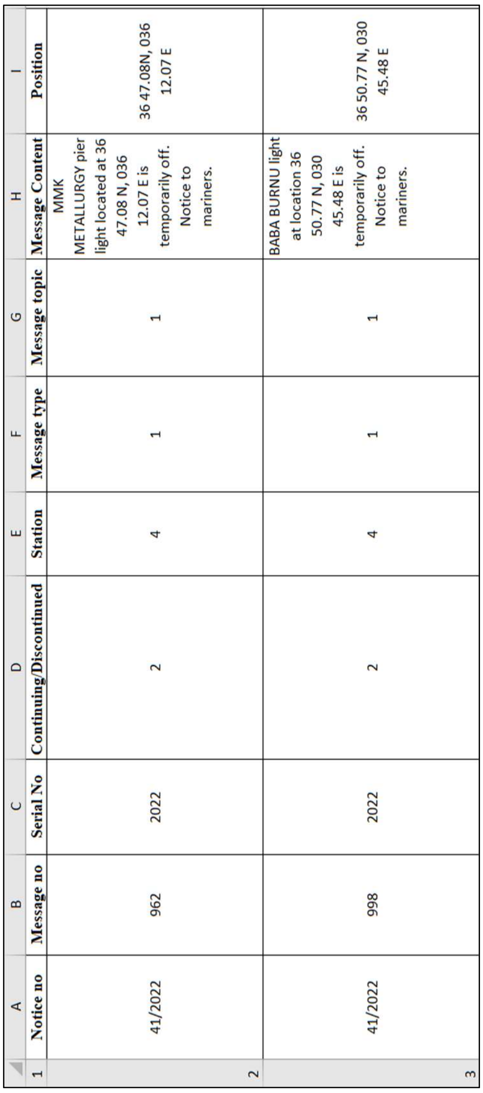
Question 2: What is the annual distribution of messages based on their topics?

Question 3: What is the annual distribution of messages based on their type?

3.3. Data analysis

The Excel screenshot in Figure 2 demonstrates the classification of data.

To find answers to the research questions mentioned in section 3.2, the data arranged in the format exemplified in Figure 2 was analyzed. There was a total of 718 data entries made for the years 2019-2022.



	A	B	C	D	E	F	G	H	I
1	Notice no	Message no	Serial No	Continuing/Discontinued	Station	Message type	Message topic	Message Content	Position
2	41/2022	962	2022	2	4	1	1	MMK METALLURGY pier light located at 36 47.08 N, 036 12.07 E is temporarily off. Notice to mariners.	36 47.08N, 036 12.07 E
3	41/2022	998	2022	2	4	1	1	BABA BURNU light at location 36 50.77 N, 030 45.48 E is temporarily off. Notice to mariners.	36 50.77 N, 030 45.48 E

Fig. 2. Example screenshot for data classification in Excel file

4. FINDINGS

Figure 3 presents the distribution of the number of messages by year as the answer to research question number 1.

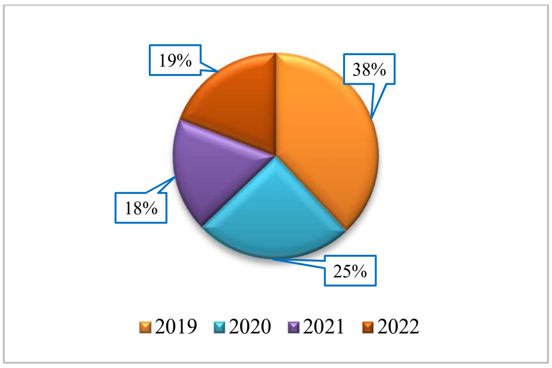


Fig. 3. The number of messages by year

Out of 718 messages, 271 (38%) was from 2019. 180 (25%) was from 2020, 129 (18%) was from 2021, and 138 (19%) was from 2022. The number of messages received was the highest in 2019. The number of messages decreased in 2020, and reached its lowest value in 2021. There is a slight increase in the number of messages in 2022 compared to 2021.

Figure 4-8 represents the annual distribution of messages based on their topics as the answer to research question number 2.

The number of messages about the first message topic, aids to navigation, is shown in Figure 4 in a year-by-year distribution.

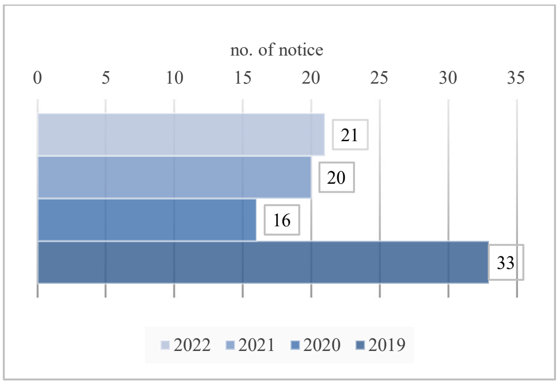


Fig. 4. The number of messages about aids to navigation by year

The most messages about navigation aids were received in 2019. The number of messages decreased by almost half in 2020, but it began to increase in 2021 and 2022.

In 2019, the topics that received the most messages were those related to temporarily extinguished or destroyed lighthouses and extinguished/broken light buoys.

The Mersin Vessel Traffic Service system activation announcement was among the messages made in this year. The messages transmitted in 2020 were about extinguished lights and buoys. Warnings about removed or installed buoys, extinguished or malfunctioning lights, and advice to stay alert for sea pollution were included in messages sent in 2021. Warnings were made in 2022 regarding the extinguished/installed lighthouses/light buoys. The distribution of messages about the second message topic, shipwrecks and floating objects, by year is shown in Figure 5.

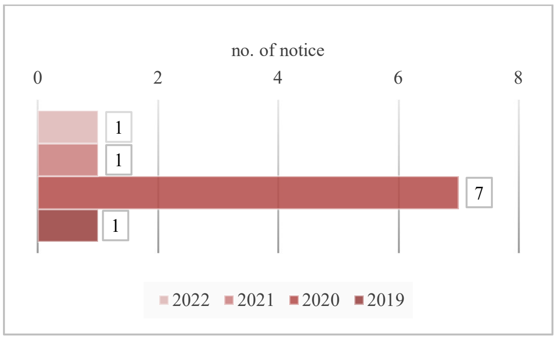


Fig. 5. The number of messages about shipwrecks and floating objects by year

In 2020, the number of messages about shipwrecks and floating objects was the highest. The evaluation of all years shows that 2 out of 10 messages were related to shipwrecks, while the remaining ones were related to floating pipes/discharge pipes.

The distribution of messages related to underwater work and research activities which is the third message topic is shown in Figure 6.

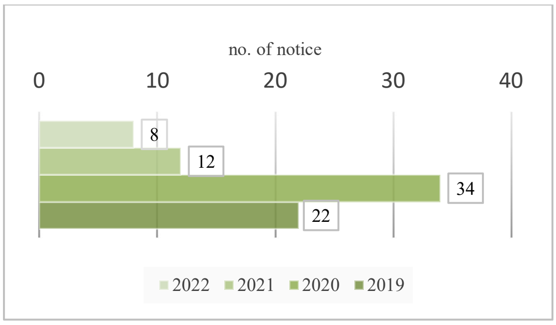


Fig. 6. The number of messages related to underwater work and research activities by year

Figure 6 shows that the most messages were transmitted in 2020. Issues like sea measurement studies, pipeline repair, underwater device backup, drilling work, seismic research, and cable repair were addressed in the messages. It has been observed that the number of messages decreased after 2020. When all years were evaluated together, it was found that the majority of messages were related to drilling and seismic research.

Figure 7 shows how messages related to drills and military activities, which is the fourth message topic, are distributed over the year.

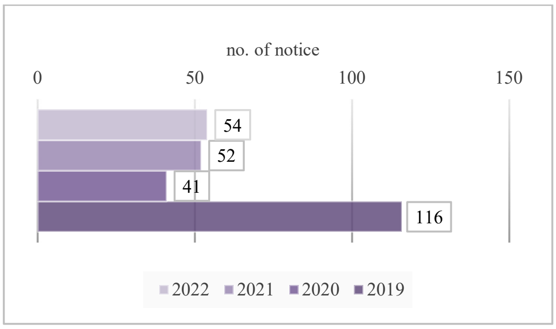


Fig. 7. The number of messages related to military activities and drills by year

The majority of messages were issued in 2019, as shown in Figure 7. It is believed that Türkiye's increase in energy resource activities in the Mediterranean Sea in 2019 is a factor in this result. In other years, it has been observed that the number of messages decreased by approximately half.

Moreover, after examining all the data, no messages were found regarding piracy and mine issues, which are the fifth and sixth message topics, respectively.

The number of messages published on other topics, which is the last message topic, is shown in Figure 8 in a year-by-year distribution.

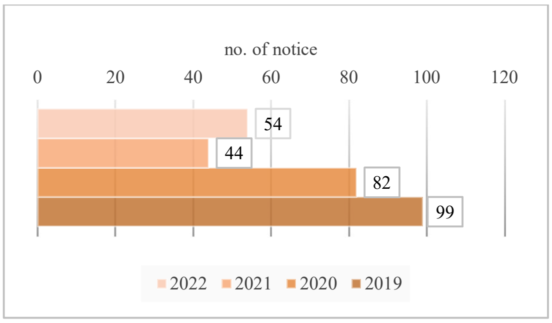


Fig. 8. The number of messages published on other topics by year

The content of the messages in Figure 8 is related to broadcasts from Turkish NAVTEX stations. The number of messages was highest in 2019, but they have decreased over the years.

An answer to research question 3 regarding the annual distribution of messages based on their type has been sought. It is seen that, all messages published between 2019 and 2022 that were examined within the scope of this study were classified as 'Navigational Warnings (A)', with code '1.' Messages under the types Meteorological Warnings (B), Ice Warnings (C), Search and Rescue Activities and Piracy (D), Weather Forecast (E) and Pilotage (F), numbered with codes 2, 3, 4, 5, 6 respectively, were not broadcast from Antalya NAVTEX Station during this date range.

Out of the 718 messages reviewed, 60 are continuing messages with repeated broadcasts, and 658 are discontinued messages. When we examine the content of the continuing messages published in the navigation area, it is seen that

- 29 messages were related to information and country policy.
- 11 messages were received about problems with navigation aids.
- There is 1 message about the shipwreck.
- There were 9 messages about platforms and drilling activities.
- 7 messages were related to drill/training and military activities,
- There were 3 messages regarding underwater work

It was determined that approximately half of the continuing messages were warning messages to other countries, while the other half were scattered among other data.

3. CONCLUSION

Every year, marine and ship technologies are being developed. This is resulting in the integration of new systems into ships. NAVTEX messages are still crucial for navigation safety. Although connecting NAVTEX with other devices on the bridge may seem to bring a complex experience in terms of use, it makes the job of officers responsible for navigational safety much easier.

Analysis of NAVTEX messages provides an important data source for the navigational safety of ships in the region. In this study, it was aimed to present that navigational risk trend in the region could be revealed by analyzing NAVTEX messages. It was assessed that using big data analysis approach to review NAVTEX messages would increase navigational safety. Therefore, the NAVTEX warnings for the Mediterranean Sea included in the notice to mariners bulletin published by the Turkish Navy Forces Office of Navigation Hydrography Oceanography between 2019 and 2022 were examined. The examination was limited to messages broadcast from Antalya station. It is aimed to find an answer to the research questions about the topics on which messages are published most, what the type of messages are and the annual change in the number of messages.

The total number of data entries made for the years 2019-2022 was 718. Out of 718 messages, 38% was from 2019, 25% was from 2020, 18% was from 2021, and 19% was from 2022. The study found that 'Navigational Warnings' was the only type of message that was published between 2019 and 2022.

The data also assessed according to the topics of warnings. The first message topic was aids to navigation. The year 2019 saw the highest number of messages about aids to navigation. The introduction of the VTS system in the region in 2019, the number of military activities and the intense warnings made about the Turkish NAVTEX system, shows that action has been taken in terms of both safety and security in the navigation area by Türkiye. In 2019, the messages were related to temporarily extinguished or destroyed lighthouses and extinguished/broken light buoys. The messages transmitted in 2020 were about extinguished lights and buoys. The warnings announced in 2021 were about removed or installed buoys, extinguished or malfunctioning lights, and advice to stay alert for sea pollution. The warnings transmitted in 2022 were about the extinguished/installed lighthouses/light buoys.

The second message topic was shipwrecks and floating objects. The number of messages about shipwrecks and floating objects was the highest in 2020. It was found that 2 out of 10 messages were related to shipwrecks, while the remaining ones were related to floating pipes/discharge pipes.

The third message topic was underwater work and research activities. The most messages under this topic were transmitted in 2020. Sea measurement studies, pipeline repair, underwater device backup, drilling work, seismic research, and cable repair were addressed in the messages. Drilling and seismic research were the most mentioned message content under this topic. The number of messages decreased after 2020.

The fourth message topic was drills and military activities. The majority of messages were sent during 2019. Turkey's increase in energy resource activities in the Mediterranean Sea in 2019 is believed to be a factor in this outcome. The number of messages has decreased by approximately half in other years.

Upon examination of the fifth and sixth topics, namely piracy and mine, it was discovered that no messages were published on these topics.

The latest message topic, namely other messages, was examined and it was discovered that the number of messages was the highest in 2019, but they have decreased over the years.

The analysis of aggregated NAVTEX messages was observed as a useful tool for providing information to ships, shipping companies, and policy makers. It is possible to ensure the navigational safety of ships navigating in the Mediterranean Sea and to make it more navigable through new systems that can be created in the light of the collected data.

This study will fill a significant gap in the literature since there has been no such a study on the Mediterranean Sea yet and there is not sufficient content on this subject in the literature. One of the limitations of this study is that it only examined data between 2019 and 2022. The time period can be extended in future studies. Another limitation is that only Antalya station's data is used. For future studies, the study area can be expanded by including warnings transmitted by other countries in the Mediterranean region. Working with a larger data set in different sea areas can lead to more detailed information in future studies. In addition, it is possible to examine and evaluate both NAVTEX and NAVAREA notices together. Through the collection and analysis of NAVTEX data on other sea areas, the captains, the shipping companies and the policy makers will benefit from the trends and potential risks obtained from the evaluation of the big data sets. A snapshot of the navigation area can be provided by big data analysis. Seafarers will be able to take proper precautions early to ensure safe navigation. Data analysis can help determine the risk distribution in certain regions by revealing the frequency of important events occurring in the region. The potential geographical distribution of these events can be determined by analyzing position information, too. Historical data analysis will allow us to determine if there is a situation that necessitates precautions in the region. The decision-making processes of shipping companies will benefit from the big data analysis.

REFERENCES

Baltacı, A. (2019). "Nitel araştırma süreci: Nitel bir araştırma nasıl yapılır?" [The Qualitative Research Process: How to Conduct a Qualitative Research?]. *Ahi Evran Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, Vol. 5, No. 2, pp. 368-388.

Borisova, L. F., Milkin, V. I., and Kholodov, G. G. (2020). "Shipping Safety in the Arctic." In *IOP Conference Series: Earth and Environmental Science, Vol. 539, 5th International Conference "Arctic: History and Modernity" 18-19 March 2020, Saint-Petersburg, Russia,* IOP Publishing, pp. 012126, DOI:10.1088/1755-1315/539/1/012126

Bowen, G. A. (2009). "Document analysis as a qualitative research method." *Qualitative Research Journal*, Vol. 9, No. 2, pp. 27-40.

Kaptan, M., Ugurlu, O. (2022). "Elektronik seyir cihazlarının deniz kazalarına etkileri". [The effects of electronic navigation devices on marine accident occurrences]. Aquatic Research, 5(1), 89-98.

Kedikli, U., and Çalağan, Ö. (2017). "Enerji alanında bir rekabet sahası olarak Doğu Akdeniz'in önemi." [The Importance of Eastern Mediterranean as a Rivalry Area in the Field of Energy]. Sosyal Bilimler Metinleri, Vol. 2017, No. 1, pp. 120-138.

Kiral, B. (2020). "Nitel bir veri analizi yöntemi olarak doküman analizi." [Document analysis as a qualitative data analysis method]. *Siirt Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, Vol.8, No. 15, pp. 170-189.

Korcz, K. (2011). "Yesterday, today and tomorrow of the GMDSS." *TransNav, International Journal on Marine Navigation and Safety of Sea Transportation*, Vol. *5, No.* 4, pp.453-459.

Korcz, K. (2016). "Communication systems for safety and security of ships." *Journal of KONES*, Vol. 23, No. 1, pp. 153-160.

Lee, S., and Lee, J. W. (2013). "An implementation of NAVTEX application on android mobile device." *In 2013 International Conference on Information Science and Applications (ICISA)*, Suwon, pp. 1-3. DOI: 10.1109/ICISA.2013.6579502

Liu, H., Liu, Z., Wang, X., and Cai, Y. (2018). "Bayes' Theorem based maritime safety information classifier." *Proc., 2018 Chinese Control and Decision Conference (CCDC),* IEEE. Shenyang, China, pp. 2725-2729. https://ieeexplore.ieee.org/abstract/document/8407588

Oğurlu, E., & Özsağlam, M. T. (2022). "Reflections on the Sovereignty Dispute for Hydrocarbon Resources in the Eastern Mediterranean." In M. T. Özsağlam (Ed.), *Politics, Economy, Security Issues Hidden Under the Carpet of Mediterranean*, European Publisher. pp. 1-29. DOI: 10.15405/BI.20221101.1

Oral, F. (2021). "Is the Crisis in the Eastern Mediterranean: Is it About Energy or Sovereignty?" *Uluslararası Kriz ve Siyaset Araştırmaları Dergisi*, Vol.5, No. 1, pp. 219-247.

Safety4sea, https://safety4sea.com/hephaestus-grounding-linked-to-inadequate-safety-policies/ [Accessed 15 December 2023].

Şen, O. and Açıkgöz, C. (2022). "Türkiye'nin Doğu Akdeniz'i Güvenlikleştirme Üçgeni: Söylemler, Görseller, Eylemler." [Turkey's Eastern Mediterranean Securitization Triangle: Discourses, Images, Actions]. *Alternatif Politika,* Vol. 14, No. 1, pp. 142-175. DOI: 10.53376/ap.2022.05

Yao, J., Liu, F., and Zhang, W. (2017). "Design of the Exciter of Weather Fax Chart and NAVTEX Message." *Procedia Computer Science*, Vol. 107, pp. 685-690. DOI: 10.1016/j.procs.2017.03.148

Žanić Mikuličić, J., Kasum, J., and Jugović, A. (2018). "Distribution of maritime safety information and improvement measures for safety of navigation." *NAŠE MORE: znanstveni časopis za more i pomorstvo*, Vol. 65, No.3, pp. 164-168.

Mersin University Journal of Maritime Faculty

Mersin University Journal of Maritime Faculty (MEUJMAF)
Vol. 5, Issue 2, pp. 45-52, December 2023
e-ISSN 2687-6612, Türkiye
DOI: 10.47512/meujmaf.1403065
Research Article

ABRASIVE WEAR BEHAVIOR OF FUNCTIONALLY GRADED AIB$_2$/AI COMPOSITE

Ömer Savas [1], İlknur Keskin Öner *[2]

[1] Yildiz Technical University, Faculty of Naval Architecture and Maritime, Departmant of Marine Engineering, İstanbul, Türkiye
ORCID ID 0000 – 0001 – 7454 – 1457
osavas@yildiz.edu.tr

[2] Yildiz Technical University, Faculty of Naval Architecture and Maritime, Departmant of Marine Engineering, İstanbul, Türkiye
ORCID ID 0000 – 0003 – 1584 – 4479
keskin@yildiz.edu.tr

* Corresponding Author

Received: 11/12/2023 Accepted: 26/12/2023

ABSTRACT

Functionally graded composites (FGM) can combine high surface wear resistance and high toughness. For this reason, it has been seen to be preferred in many regions, especially in the defense and maritime sectors, in recent years. This study is an experimental study on the investigation of the wear properties of functionally graded AlB$_2$ boride reinforced composite materials, which can be an alternative in the manufacturing of ship machinery parts exposed to repeated loads and wear. This study aims to increase the industrial usability of the boron element, which has strategic importance for our country. Pin-On-Disk technique and abrasive wear method were used to determine the wear properties of composites. In the wear tests, a total of 5 factors consisting of wear factors such as the region of the composite (% reinforcement ratio), abrasive particle diameter, application load, sliding distance and sliding speed were selected as test parameters with 3 levels. In wear tests, the "Taguchi Experimental Design" method was used. As a result of the study, it was seen that the hardness and wear resistance of aluminum increased with the addition of AlB$_2$ into the aluminum matrix. It was observed that the load had an effect of 33.98%, the abrasive particle diameter had an effect of 31.68% and the AlB$_2$ reinforcement ratio had a 10.73% effect on the wear resistance of the composites. As a result of the study, linear equations predicting 'wear resistance in different conditions' were obtained.

Keywords*: Wear, AlB$_2$, Functionally Graded Composite*

1. INTRODUCTION

Composite materials are defined as a new type of material created by combining two or more different materials at a macro level and they carry the best properties of the materials that form them(Miracle 2006; Rohatgi and Paper 2001; Pramod et al. 2015; Kumar et al. 2008). In general, metal matrix composites consist of a matrix with low strength and ductility and a reinforcement material with high hardness and wear resistance. The need for lightweight and high-performance metals has paved the way for the research and development of Aluminum Matrix Composites.

Compared to conventional aluminum alloys, aluminum matrix composites have high specific strength, superior wear resistance and stability at high temperatures (Rosso 2006; Kane et al. 2016; Radhika and Raghu 2018). Silicon carbide (SiC) and Alumina (Al_2O_3) are preferred as strengthening phases due to their high wettability by aluminum and their low prices (Ozdin 2007). The development and discovery of new production processes have shown that there are various ceramic and intermetallic reinforcers with high potential for Aluminum Matrix Composites (Tjong and Ma 2000; Ma et al. 1999). The mechanical properties of composite materials increase with increasing reinforcement ratio and increasing aspect ratio (width/thickness ratio of the reinforcement phase) (Kayikci and Savaş 2015; Tjong and Mai 2008).

There are very limited studies on aluminum matrix AlB_2 boride reinforced composite materials (Kayikci and Savaş 2015; Deppisch et al. 1997). AlB_2 reinforced composites can be produced easily and cheaply with the in-situ production method. Since it is produced with this method, it exhibits a number of superior properties desired in composite production, such as wettability, homogeneous distribution, thermodynamic stability and high aspect ratio (length/thickness) (Hall and Economy 2000; Deppisch et al. 1997). Boric acid (H_3BO_3), boric oxide (B_2O_3), borax ($Na_2B_4O_7.10H_2O$), potassium chloride and commercial Al-B master alloys are used as boron source in the production of AlB_2 composites (Kayikci and Savaş 2015; Hall and Economy 2000). Commercial Al-B alloys are widely used as grain refiners in the casting of aluminum alloys and in the production of conductive wires with high conductivity.

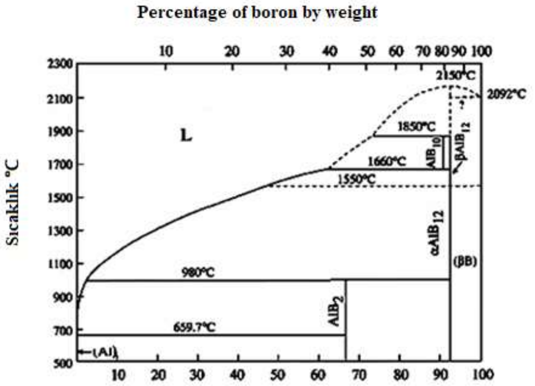


Figure.1. Al–B binary phase diagram [16]

In order to produce AlB_2 boride reinforced composites properly, the Al-B phase diagram must be well understood (Hall and Economy 2000; Hall and Economy 2000). As can be seen in the phase diagram given in Fig. 1, it is seen that the boron element does not dissolve in aluminum at room temperature and exists in the form of AlB_{12} and AlB_2 boride compounds. Additionally, it is seen that the Al-B phase diagram has a peritectic reaction line at approximately 980°C. It is noteworthy that AlB_{12} boride structures are stable above the peritectic reaction temperature and AlB_2 below it. While AlB_2 boride structures have high aspect ratio and high mechanical properties, AlB_{12} boride structures are coaxial, unstable at room temperature, brittle and have low mechanical properties. For this reason, AlB_{12} is not desired to be present in the structure in the production of boride structured composites.

In functionally graded composites (FGM), the reinforcement ratio varies from the inner region to the outer region of the mold. For this reason, the physical and mechanical properties of composites vary depending on the change in reinforcement ratio (Kayikci and Savaş 2015; Melgarejo et al. 2008; Naebe and Shirvanimoghaddam 2016; Nadu 2016). FGM can combine high surface wear resistance and high toughness (Karun 2017).

Tjong and Lau (2000) showed that the wear resistance increased dramatically with the increase in the proportion of reinforcement particles in the composite. In their study to investigate the abrasive wear behavior of functionally graded TiB_2 reinforced aluminum matrix composites, Savaş et al. (2020) reported that the weight losses of the composites increased with increasing load and sliding speed, and that the weight losses decreased significantly with increasing reinforcement ratio.

Radhika and Raghu (2016) examined the abrasive wear behavior of functionally graded AlB_2/Al composites. In the study, the effects of test parameters such as load, sliding distance and abrasive type (SiC and Al_3O_2) on the wear behavior of composites were examined. Wear test results showed that the wear rate decreased with increasing AlB_2 reinforcement ratio in the aluminum matrix and SiC particles had more abrasive properties.

Previous studies conducted to investigate the wear behavior of AlB_2/Al composites reported that wear resistance increased with increasing AlB_2 reinforcement ratio in the aluminum matrix (Ficici, 2016; Ficici and Koksal, 2016; Ficici et al., 2011).

For wear tests, functionally graded AlB2 reinforced aluminum matrix composites, which were produced and characterized in our previous study, were used (Savaş and Karataş 2022). In another previous study, the wear behavior of these composites was examined in a limited way (Öner and Savaş, 2022). In this study, the wear behavior of composites was examined by using more comprehensive and more advanced analysis techniques in order to take previous studies to a further stage.

2. EXPERIMENTAL STUDIES

2.1. Composite Production and Characterization

Wear test samples measuring 10x10x20 mm were taken to be used in wear tests. When looking at the cross-sectional image of the test sample, it can be seen that it has two regions in the direction of spinning, one reinforced with AlB_2 and one that is not reinforced. In the previous study, wear experiments were conducted separately on these two region. In order to determine the regional wear behavior of the composite, the reinforced region in the direction of blowing was divided into two. As seen in Fig. 2, the region corresponding to the outside of the mold is named A, and the inner region (the part between region A and the unreinforced region C) is named B.

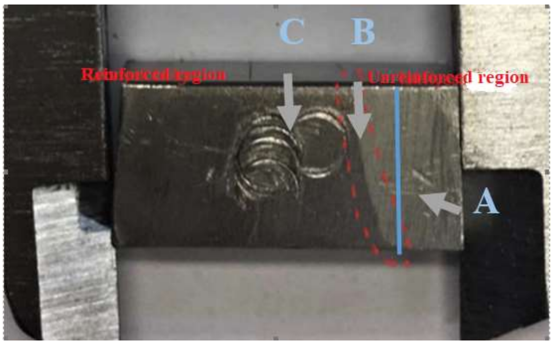


Figure 2. Wear test sample

In order to speed up the wear process, abrasive wear technique was used in the wear analysis of composites. Abrasive wear tests of composites were carried out with the 'Pin-On-Disk' method given in Fig. 3 (Melgarejo, 2008). Fig. 3 shows that the abrasive media is placed on the disc and the composite pin is pressed onto the abrasive media by the applied load. In abrasion tests, the weights of the samples before and after the test were measured with a scale with a sensitivity of 0.0001 g, and the wear amounts were determined by taking the difference of these measurements. The average wear resistance of each test recipe was calculated by considering the weight losses.

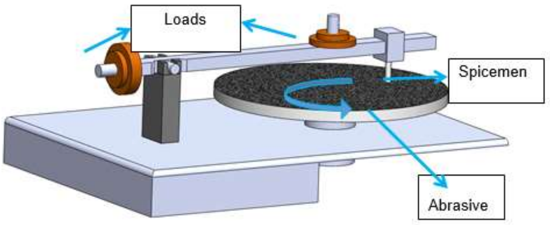


Figure 3. Schematic representation of the experimental setup

Water sandpapers of 1000, 1200 and 1500 grit with particle sizes of 18, 15 and 12 µm were determined as the abrasive medium. Wear tests were carried out at a sliding distance of 100-200-300 meters, at sliding speeds of 1-3-4.5 m/s and under 1-2-3 N loads. Factor and level values determined for wear tests are given in Table 1 considering the factors and levels given in Table 1, if all combinations are tried, a total of '3x3x3x3x3' = 243 experiments are required. Although conducting such a large number of experiments is negative in terms of cost and time, conducting too many experiments means making too many mistakes. For this reason, Taguchi experimental approach was used in this study.

Table 1. Factors selected for wear tests and their level abrasive medium particle size

	Factor	Factor level		
		Level 1	Level 2	Level 3
A	Region % AlB_2 ratio	0,0 (Region C)	5,0 (Region B)	7,5 (Region A)
B	Abrasive Particle size, µm	18	15	12
C	Load, N	1	2	3
D	Sliding speed, m	100	200	300
E	Sliding distance, m/s	1,0	3,0	4,5

The Taguchi method, which is preferred to improve a process or a system with a small number of trials, was developed by Dr. Genichi Taguchi in the 1950s. It is an effective design method for product quality, customer satisfaction and pre-production planning. The Taguchi method has been used effectively in many studies conducted to examine the wear behavior of materials (Unal et al., 2008; Melgarej, 2018; Koksal et al., 2014.

As a result of the preliminary examinations made according to the Taguchi approach, it was seen that the most suitable series for the factors and levels given in Table 1 was the L_{27} orthogonal series. In Table 2, 27 experimental prescriptions determined by considering the $L_{27}{}^{(35)}$ orthogonal series are given.

Table 2. $L_{27}{}^{(35)}$ orthogonal series and test recipes selected for wear experiments

Test number	% AlB_2 ratio	Load, N	Abrasive particle diameter, µm	Speed, m/s	Distance, m
	A	B	C	D	E
1	7,5	1	18	1	100
2	7,5	1	15	3	200
3	7,5	1	12	4,5	300
4	7,5	2	18	3	200
5	7,5	2	15	4,5	300
6	7,5	2	12	1	100
7	7,5	3	18	4,5	300
8	7,5	3	15	1	100
9	7,5	3	12	3	200
10	5	1	18	3	300
11	5	1	15	4,5	100
12	5	1	12	1	200
13	5	2	18	4,5	100
14	5	2	15	1	200
15	5	2	12	3	300
16	5	3	18	1	200
17	5	3	15	3	300
18	5	3	12	4,5	100
19	0	1	18	4,5	200
20	0	1	15	1	300
21	0	1	12	3	100
22	0	2	18	1	300
23	0	2	15	3	100
24	0	2	12	4,5	200
25	0	3	18	3	100
26	0	3	15	4,5	200
27	0	3	12	1	300

Wear tests were carried out in a way to minimize environmental and systemic errors, taking into account the 27 different test recipes given in Table 2. Each experimental recipe was repeated at least three times in order to minimize systemic and environmental errors.

3. RESULTS

In Fig. 4 (A, B and C regions), SEM images of AlB_2 reinforced and non-reinforced regions are given. Approximately 30 µm long AlB_2 structures are seen in AlB_2 reinforced regions. It is also noteworthy that there is no intermetallic compound between the matrix and AlB_2 boride structures. It is noteworthy that there is no significant difference in terms of AlB_2 reinforcement ratio between regions A and B. However, it is clearly seen that there are no AlB_2 boride structures in the unreinforced regions. As a result of the SEM analysis, no significant micro porosity was found in both reinforced and unreinforced regions.

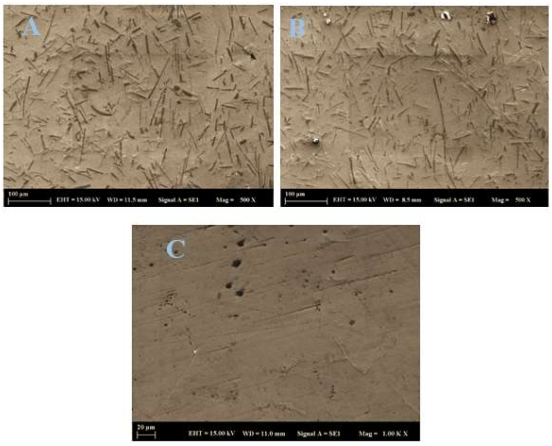

A
100 µm EHT = 15.00 kV WD = 11.5 mm Signal A = SE1 Mag = 500 X
B
100 µm EHT = 15.00 kV WD = 8.5 mm Signal A = SE1 Mag = 500 X
C
20 µm EHT = 15.00 kV WD = 11.0 mm Signal A = SE1 Mag = 1.00 K X

Figure 4. SEM image of a) A region, b) B region and c) C region of the composite material to be subjected to wear

The % AlB_2 ratio, density and hardness values of the composite regions to be exposed to AlB_2 wear are given in Table 3.

Table 3. Composite material properties

Region	Reinforcement ratio	Density,gr/cm^3	Hardness, HB
A	%7,5	2,72	79,17
B	%5,0	2,71	55,05
C	%0,0	2,70	45,05

In Table 3, it is seen that the AlB_2 reinforcement ratio in the reinforced region of the composites varies between 7.5% and 5%. Additionally, the table shows that the density and hardness values of the composite increased with increasing AlB_2 in the aluminum matrix. The table shows that the highest hardness value was measured as 79.17 HB in the region reinforced with 7.5% AlB_2.

Table 4 shows the wear resistance results obtained as a result of the wear tests of 27 test recipes. The last column of the table shows the S/N ratios of the wear results calculated according to the "highest is best" quality characteristic. In the experiments carried out in the table, it is seen that the wear resistance values vary between 35400 m/g and 2290 m/g. The highest abrasion resistance was observed as 14181 m/g on average in the 2nd test recipe. The lowest abrasion resistance was observed in the 22nd test recipe with 2417 m/g. It is noteworthy that, in general, the wear resistance of regions with low reinforcement ratio is low, while it is higher in regions reinforced with AlB_2. Additionally, the table shows that S/N ratios vary between 91.9 dB and 67.7 dB.

Table 5 shows the ANOVA table prepared taking into account S/N ratios. The sum of squares, variance, F and P values of each factor and its interactions are given in the Table 5. Statistically, P values in the ANOVA table below 0.05 indicate that that factor is effective, while values above 0.05 indicate that it is not effective. The table shows that load, abrasive particle diameter and reinforcement ratio are effective on the wear of composites. It shows that sliding speed, distance and factor interaction are not important. When looking at the percentage effects of the factors on wear, it is seen that the load factor has the highest effect with 33.98%, followed by the abrasive particle diameter factor with 31.68% and the Reinforcement ratio factor with 10.73%. It is seen that the sliding speed factor, which does not have a significant effect, has an effect of 3.36% and the sliding distance factor has an effect of 0.45%. It shows that uncontrollable factors on wear have a total effect of 19.8%.

Fig. 5 shows the 'main effect graph' drawn for wear resistance. The graph shows the wear resistance changes with the factor level change of each factor. In the graph, the factor level that gives the highest wear resistance value shows the optimum test conditions. Accordingly, it shows that the highest wear resistance of composites can be achieved by abrading the regions with 7.5% reinforcement ratio under 1 N load, in an abrasive particle environment of 12 µm diameter, at a sliding speed of 4.5 m/s and at a sliding distance of 200 m. However, it should be noted that speed and road factors do not have a significant effect here. According to Fig. 5, the optimum test recipe is $A_3B_1C_1D_3E_2$.

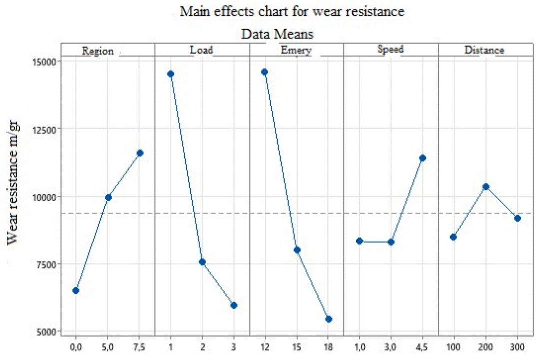


Figure 5. Key effects graphs for wear resistance

Table 4. Experimental prescriptions and wear resistance results and their S/N ratio

No	% AlB_2 ratio	Load, N	Abrasive particle diameter,µm	Speed, m/s	Distance, m	1. Measuring m/gr	2. Measuring m/gr	3. Measuring m/gr	Average wear resistance, m/gr	S/N ratio, dB
1	7,5	1	18	1	100	11656	8272	11652	10526,7	80,1
2	7,5	1	15	3	200	14181	14170	14192	14181,0	83,0
3	7,5	1	12	4,5	300	42269	35400	42268	39979,0	91,9
4	7,5	2	18	3	200	5941	5053	4677	5223,7	74,2
5	7,5	2	15	4,5	300	6784	6038	4684	5835,3	75,0
6	7,5	2	12	1	100	8843	7542	8852	8412,3	78,4
7	7,5	3	18	4,5	300	3500	3087	3351	3312,7	70,4
8	7,5	3	15	1	100	4346	4838	4931	4705,0	73,4
9	7,5	3	12	3	200	12929	10722	12932	12194,3	81,6
10	5	1	18	3	300	8792	8795	8779	8788,7	78,9
11	5	1	15	4,5	100	10990	10775	10760	10841,7	80,7
12	5	1	12	1	200	16027	18506	16027	16853,3	84,5
13	5	2	18	4,5	100	3663	4995	6106	4921,3	73,3
14	5	2	15	1	200	19726	17860	19726	19104,0	85,6
15	5	2	12	3	300	7327	7341	8454	7707,3	77,7
16	5	3	18	1	200	2290	2699	2397	2462,0	67,8
17	5	3	15	3	300	3461	4778	4352	4197,0	72,2
18	5	3	12	4,5	100	16652	16648	10990	14763,3	82,9
19	0	1	18	4,5	200	10368	8326	8335	9009,7	79,0
20	0	1	15	1	300	5028	5035	5018	5027,0	74,0
21	0	1	12	3	100	14653	16281	16182	15705,3	83,9
22	0	2	18	1	300	2419	2410	2424	2417,7	67,7
23	0	2	15	3	100	3960	4627	3960	4182,3	72,4
24	0	2	12	4,5	200	9314	12211	9425	10316,7	80,1
25	0	3	18	3	100	2376	2365	2836	2525,7	68,0
26	0	3	15	4,5	200	3434	3536	5132	4034,0	71,7
27	0	3	12	1	300	5575	5469	5602	5548,7	74,9

Table 5. ANOVA tables

Factors	Column	DF	Seq SS	Adj SS	Adj MS	F	P	Contribution
Reinforcement ratio	A	2	88,22	88,22	44,112	4,61	0,047	10,73%
Load	B	2	314,68	314,7	157,34	16,43	0,001	33,98%
Abrasive particle diameter	C	2	333,22	333,2	166,61	17,4	0,001	31,68%
Speed	D	2	20,16	20,16	10,078	1,05	0,393	3,36%
Distance	E	2	34,45	34,45	17,224	1,8	0,226	0,45%
Region*Load		4	34,42	34,42	8,605	0,9	0,508	
Load*Emery		4	55,39	55,39	13,849	1,45	0,304	
Residual Error		8	76,59	76,59	9,574			19,80%
Total		26	957,14					100,00%

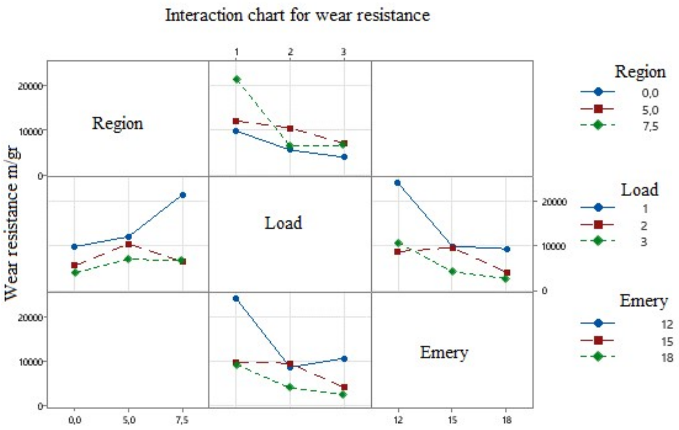


Figure 6. Interaction graphs for wear resistance

In the graph in Fig. 6, the relationships between the Reinforcement Ratio-Load and Abrasive Particle Diameter (sandpaper)-Load factors were examined, but it was observed that there was no significant relationship.

In this study, test recipe number 3 in Table 4 has the optimum test recipe (A3B1C1). Therefore, instead of conducting an extra experiment, the results of experiment number 3 were used for validation experiments. The average S/N ratio, estimated confidence interval and verification experiment average S/N ratios calculated according to optimum conditions are given in Table 6.

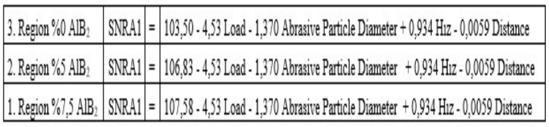
Table 6. Predictive and verification test results

Quantity	Results
Optimum experimental conditions	A3B1C1
Estimated average S/N ratio	92,1 dB
Confidence interval for α= 0,05	91,0 $< \mu <$ 94,2 dB
Verification test S/N ratio	91,9 dB

In Table 6, the S/N ratio of the verification test result is 91.9 dB. This value is within the estimated confidence interval calculated as seen in the table. This result shows that the experiments were carried out correctly.

As a result of the statistical analysis, a linear regression equation was prepared for each region of the composite material (Table 7). Thanks to this equation, the wear resistance of the composite material can be predicted under predetermined wear conditions.

Table 7. Regression equations



3. Region %0 AlB_2	SNRA1	=	103,50 - 4,53 Load - 1,370 Abrasive Particle Diameter + 0,934 Hız - 0,0059 Distance
2. Region %5 AlB_2	SNRA1	=	106,83 - 4,53 Load - 1,370 Abrasive Particle Diameter + 0,934 Hız - 0,0059 Distance
1. Region %7,5 AlB_2	SNRA1	=	107,58 - 4,53 Load - 1,370 Abrasive Particle Diameter + 0,934 Hız - 0,0059 Distance

In order to test the regression equation, the wear resistance value and S/N ratios that would occur under spesific wear conditions were calculated. Estimated wear resistance values and S/N ratios are given in Table 8.

Table 8. Control test recipes and test results

Reinforcement ratio, %	Load, N	Abrasive particle size, µm	Speed, m/s	Distance, m	S/N ratio	Wear resistance m/gr
7,5	1	12	4,5	100	88,93	23258,4
0	1	12	4,5	100	84,86	18191,4
7,5	1	12	4,5	200	90,50	25124,5

In order to thin the wear surfaces of the composites, the composite regions reinforced with 0% and 7.5% AlB_2 were exposed to wear under equal conditions under a load of 1 N, in an abrasive particle environment of 12 µm diameter, at a sliding speed of 4.5 and at a sliding distance of 100 m.

Fig. 7 shows the worn surface SEM image of the unreinforced region, and Fig. 8 shows the worn surface SEM image of the region reinforced with 7.5% AlB_2. When the surface images are examined, deep wear marks and material losses as a result of plastic deformation are observed in the worn surface image of the undisturbed region. On the other hand, in the worn surface image of the reinforced region strengthened with 7.5% AlB_2, it is seen that the wear marks are few and shallow. However, no significant plastic deformation was observed on the worn surfaces of the reinforced region.

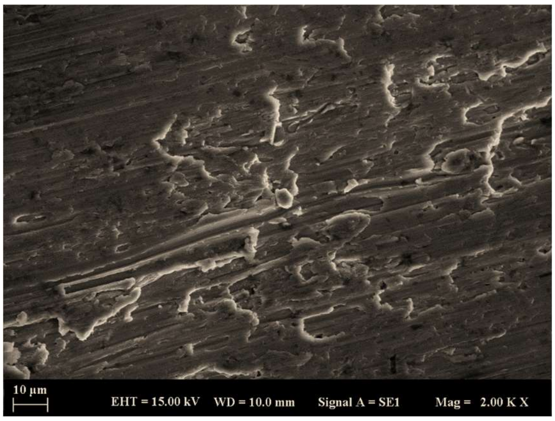


Figure 7. SEM image of the abraded surface of the not reinforced region with AlB_2

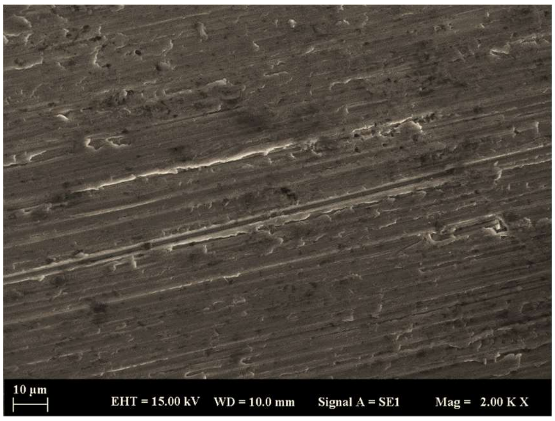


Figure 8. SEM image of the abraded surface of the reinforced region with AlB_2

4. EXAMINATION OF THE RESULTS

The 'Surface Graph' showing the change in wear resistance depending on load and reinforcement is given in Fig. 9. The graph shows that wear resistance decreases with increasing load, similar to previous studies (Pramod et al., 2015; Kumar et al., 2008; Kane et al., 2016). The probable reason for this is that the amount of wear was increased due to the increased wear and tear deterioration with the applied load, which caused the wear resistance to deteriorate.

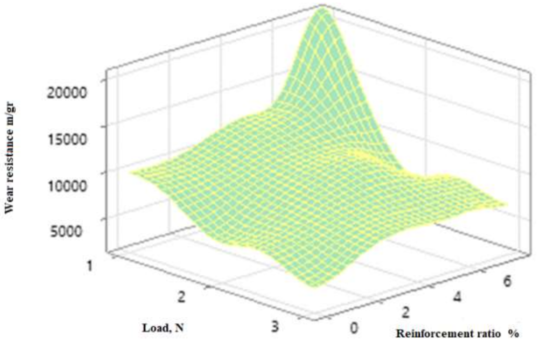


Figure 9. Wear resistance change graph depending on load and reinforcement ratio

The surface graph showing the change in wear resistance depending on the abrasive particle size and reinforcement ratio can be seen in Fig. 10. It has been reported from previous studies that wear resistance decreases with increasing abrasive particle size (Ozdin,2007; Radhika and Raghu, 2016; Radhika and Raghu, 2018). Similarly, in this study, wear resistance decreased with increasing abrasive particle diameter. The probable reason for this is that larger diameter abrasive particles have more sharp corners and therefore are more likely to penetrate the worn surfaces.

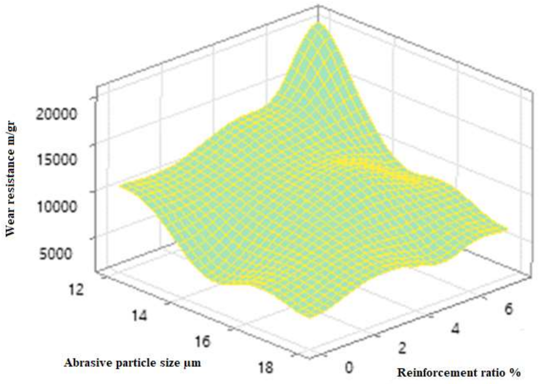


Figure 10. Wear resistance change graph depending on abrasive particle diameter and reinforcement ratio

Fig. 9 and Fig. 10 show that wear resistance increases with increasing AlB$_2$ ratio in the aluminum matrix. The reason for this is that, as can be seen in Table 1, the hardness value of the reinforced regions with AlB$_2$ is higher. Previous studies have reported that wear resistance decreases with increasing hardness value (Radhika and Raghu, 2016; Ficici, 2016**;** Kumar et al., 2008). It is thought that the reason why the wear resistance of the reinforced regions with AlB$_2$ is higher than the hardness of the unreinforced regions is due to the fact that the abrasive particles cannot penetrate the worn surfaces with the increased hardness.

5. CONCLUSION

The results we obtained in this study are summarized below;

1- It has been determined that the most effective factor on the wear resistance of functionally graded AlB2 boride-reinforced aluminum matrix composite materials for a 0.05 confidence level is the load factor, followed by the abrasive particle size and reinforcement ratio factors, respectively.

2- It was observed that sliding speed and distance factors did not have a significant effect on wear resistance.

3- In the worn surface images, it was determined that the wear marks in the unreinforced regions were deeper than in the reinforced regions with AlB$_2$.

4- It has been determined that the addition of AlB$_2$ boride particles into aluminum improves the wear resistance of the composites by 10.73%. It was observed that the applied load and the abrasive particle size had an effect on wear resistance of 33.98% and 31.68%, respectively.

5- With the Taguchi approach, a regression equation was obtained with only 27 test prescriptions instead of 243 experiments, and the wear resistance of the composites worn under different conditions was successfully predicted.

ACKNOWLEDGEMENTS

This study was supported by the project number FLO-2022-4918 of Yıldız Technical University Scientific Research Project Coordination Office. I would like to thank the Scientific Research Project Coordination Office for their support.

REFERENCES

Deppisch, C., Liu, G., Shang, J. K., & Economy, J. (1997). “Processing and mechanical r, properties of A1B2 flake reinforced Al-alloy composites,” vol. 225, no. 96, pp. 153–161.

Ficici, F. & Koksal, S. (2016). “Microstructural characterization and wear properties of in situ AlB2-reinforced Al-4Cu metal matrix composite,” *Journal of Composite Materials*, vol. 50, no. 12, pp. 1685–1696.

Ficici, F. (2016). “The experimental optimization of abrasive wear resistance model for an in-situ AlB2/Al-4Cu metal matrix composite,” *Industrial Lubrication and Tribology*, vol. 68, no. 6, pp. 632–639.

Ficici, F., Koksal, S., Kayikci, R., & Savas, O. (2011). “Investigation of unlubricated sliding wear behaviours of in-situ AlB 2/Al metal matrix composite,” *Advanced Composites Letters*, vol. 20, no. 4, pp. 109–116.

Hall, A. C., & Economy, J. (2000). “Preparing High- and Low-Aspect Ratio AlB 2 Flakes from Borax or Boron Oxide,” no. February, pp. 42–44.

Hall, A., & Economy, J. (2000). The Al (L)+ AlB12↔ AlB2 peritectic transformation and its role in the formation of high aspect ratio AlB2 flakes. *Journal of phase equilibria*, 21(1), 63-69.

Kane, S. N., Mishra, A., & Dutta, A. K. (2016). "Preface: International Conference on Recent Trends in Physics (ICRTP 2016)," *Journal of Physics: Conference Series*, vol. 755, no. 1.

Karun, A. S. (2017). Fabrication and Characterization of Functionally Graded Metal and Polymer Composites by Sequential and Centrifugal Casting Techniques, PhD Thesis, Materials Science and Technology Division CSIR-National Institute for Interdisciplinary Science and Technology (NIIST) (Formerly, Regional Research Laboratory) Council of Scientific & Industrial Research (CSIR), Govt. of India Thiruvananthapuram – 695 019 India.

Kayikci, R., & Savaş, Ö. (2015). "Fabrication and properties of functionally graded Al/AlB<inf>2</inf> composites," *Journal of Composite Materials*, vol. 49, no. 16, pp. 2029–2037.

Kayikci, R., & Savaş, Ö. (2015). "Fabrication and properties of in-situ Al/AlB2 composite reinforced with high aspect ratio borides," *Steel and Composite Structures*, vol. 19, no. 3, pp. 777–787.

Keskin Öner, İ., & Savaş, Ö. (2022). "Savurma Döküm Yöntemi ile Üretilmiş AlB2/Al Kompozit Malzemelerin Aşınma Davranışlarının İncelenmesi," *Journal of Marine and Engineering Technology (JOINMET)*, vol.2, no.1, pp.40-49.

Kök, M., & Özdin, K. (2007). "Wear resistance of aluminium alloy and its composites reinforced by Al 2 O 3 particles," vol. 183, pp. 301–309.

Koksal, S., Ficici, F., Kayikci, R., & Savas, O. (2014). "Experimental optimization in turning of in-situ AlB2 reinforced AlMg3 matrix composites produced by centrifugal casting method," *Journal of Composite Materials*, vol. 48, no. 15, pp. 1801–1812.

Kumar, S., Chakraborty, M., Sarma, V. S., & Murty, B. S. (2008). "Tensile and wear behaviour of in situ Al-7Si/TiB2 particulate composites," *Wear*, vol. 265, no. 1–2, pp. 134–142.

Melgarejo, Z. H., Suárez, O. M., & Sridharan, K. (2008). "Composites: Part A Microstructure and properties of functionally graded Al – Mg – B composites fabricated by centrifugal casting," vol. 39, pp. 1150–1158.

Miracle, D. B. (2006). "Metal Matrix Composites for Space Systems: Current Uses and Future Opportunities." vol. 175, no. 1–3, pp. 364–375.

Naebe, M., & Shirvanimoghaddam, K. (2016). "Functionally graded materials: A review of fabrication and properties," *Applied Materials Today*, vol. 5, pp. 223–245.

Rohatgi, P. (2001). Cast metal matrix composites: Past, present and future. In *Transactions of the American Foundry Society and the One Hundred Fifth Annual Castings Congress* (pp. 1-25).

Pramod, S. L., Bakshi, S. R., & Murty, B. S. (2015). "Aluminum-Based Cast in Situ Composites: A Review," *Journal of Materials Engineering and Performance*, vol. 24, no. 6, pp. 2185–2207.

Radhika, N., & Raghu, R. (2016). "Effect of Abrasive Medium on Wear Behavior of Al/AlB2 Functionally Graded Metal Matrix Composite," *Tribology Online*, vol. 11, no. 3, pp. 487–493.

Radhika, N., & Raghu, R. (2018). "Effect of Centrifugal Speed in Abrasive Wear Behavior of Al-Si5Cu3/SiC Functionally Graded Composite Fabricated by Centrifugal Casting," *Transactions of the Indian Institute of Metals*, vol. 71, no. 3, pp. 715–726.

Rosso, M. (2006). "Ceramic and metal matrix composites: Routes and properties," *Journal of Materials Processing Technology*, vol. 175, no. 1–3, pp. 364–375.

Savaş, Ö. (2020). "Application of Taguchi's method to evaluate abrasive wear behavior of functionally graded aluminum-based composite," *Materials Today Communications*, vol. 23, no. October 2019.

Savaş, Ö., & Keskin, İ. (2022). Savurma döküm yöntemi ile üretilmiş AlB2/Al kompozit malzemelerin aşınma davranışlarının incelenmesi. *Journal of Marine and Engineering Technology*, 2(1), 40-49.

Nadu, T. (2016). "Review of Centrigufal Casting of Aluminium Composites," pp. 933–935.

Tjong, S. C., & Ma, Z. Y. (2000). "Microstructural and mechanical characteristics of in situ metal matrix composites," *Materials Science and Engineering R: Reports, vol.* 29, no. 3, pp. 49–113.

Tjong, S. C., & Mai, Y. W. (2008). "Science and Processing-Structure-Property Aspects of Particulate- and whisker-reinforced titanium matrix composites," vol. 68, pp. 583–601.

Unal, H., Ficici, F., Mimaroglu, A., Demirkol, A., & Kırdar, A (2016). "Prediction and optimization of tribological behavior of nylon composites using Taguchi analysis method," *Journal of the Brazilian Society of Mechanical Sciences and Engineering*, vol. 38, no. 7, pp. 2097–2104.

MEUJMAF

Mersin University
Journal of Maritime Faculty

CONTENTS

Volume 5 – Issue 2

ARTICLES

December 2023 Volume: 5 Issue: 2