Hunting Vulnerabilities in the Maritime Domain: a Domain Wide Cybersecurity Vulnerability Analysis

Abdullah Zafar and Ahmed Amro[0000−0002−3390−0772]

Norwegian University of Science and Technology NTNU, Norway
ahmed.amro@ntnu.no

Abstract. The maritime domain, constituting over 80% of global trade, is a critical component of the world economy, facilitating the transfer of vast quantities of goods across the globe. In this way, the success of other crucial sectors vital to the normal functioning of life relies heavily on the pivotal role of the maritime domain. People have been navigating waterways through ships since ancient times. With technological progress, the structure and functioning of these ships have changed drastically. Modern ships comprise a wide array of interconnected and complicated information and operational cyber physical systems. With increasing connectivity through modern communication technologies, these systems are fast becoming connected to the outside world. Furthermore, the trend of remote-controlled and autonomous ships is expected to increase soon. Hence, assessing the cybersecurity posture of the maritime systems and identifying & fixing the vulnerabilities that comprise those ships is of utmost importance. To achieve these objectives, this research contributes in two ways, 1) proposing a comprehensive vulnerability and threat analysis methodology, named *MaThreX* developed to compile maritime-related known vulnerabilities and gather related threat-related information providing key insights to enhance decision-making and security measures, and 2) results from utilizing *MaThreX* for conducting a domain-wide analysis of the vulnerabilities found in the maritime assets and infer threat-related information to capture the threat landscape in the domain.

Keywords: First keyword · Second keyword · Another keyword.

1 Introduction

The role of the maritime domain as a critical infrastructure has invited a large body of research and interest among the domain stakeholders to invest efforts for ensuring safe and secure operations and cybersecurity has been identified as a major concern in this regard. According to a recent survey on the state of cyber risk management in the maritime industry, 44% of the 200 industry professionals surveyed reported that their organizations have been the target of a cyber attack. The survey also revealed that shipping companies pay an average of $3.1 million in ransom for cyber attacks [8]. These findings highlight the significant impact of cyber attacks on the maritime sector, making it a crucial factor for change.

In 2017, the International Maritime Organization (IMO) passed Resolution MSC. 428(98) [18] which made it mandatory for ship owners and operators to include cybersecurity in their safety management systems. The resolution was supported with guidelines for cyber risk management [4] which called for continuous risk analysis to be performed, taking into account the threat landscape including current and emerging cyber threats and vulnerabilities. The International Association of Classification Societies (IACS) released revised Unified Requirements (URs) in April 2024. These requirements include UR26 (Cyber Resilience of Ships) [6] and UR27 (Cyber Resilience of On-board Systems and Equipment) [7]. Both documents provide a set of minimum performance and functional criteria that aim to ensure that all new vessels contracted after the 1st of July 2024 are cyber-resilient. They also provide detailed requirements for evaluation and testing, incident response plans, recovery plans, and training and drills. These requirements are expected to have a significant impact on shipowners, classification societies, and manufacturers/suppliers in the maritime industry. The UR27 refers to reducing vulnerabilities through hardening and applying patches to onboard systems and equipment. On the other hand, asset vulnerabilities are a critical element in the risk assessment in the UR26. The document includes a requirement that suggests the application of vulnerability scanning for keeping up-to-date systems during the commissioning phase of ships. Additionally, it discusses the management of software updates during the operational phase by addressing vulnerabilities and cyber risks. Furthermore, there is a requirement for ship cybersecurity and resilience programs to be made to the society which considers "known vulnerabilities".

The importance of identifying, monitoring, and addressing vulnerabilities in the domain is clear and should be seen as a vital and continuous process for all involved stakeholders. While many studies have discussed vulnerabilities in the context of vulnerability scanning, analysis, threat and risk assessment, and management, none have looked at the overall cyber risk using existing Common Vulnerability and Exposures (CVEs) in the domain. Therefore, this paper aims to examine the cyber threat landscape in the maritime domain by considering existing known vulnerabilities.

Our proposed approach differs from the existing literature, which mainly focuses on threats and risks using experimental studies or theoretical scenarios. Instead, we utilize CVEs to make realistic assumptions about system risks and encompass a broad range of them in the maritime domain. This approach will assist various stakeholders in understanding the threat landscape better and offer insights to enhance defences in the maritime domain.

Our methodology which is supported by a tool called Maritime Threat eXplorer (MaThreX), relies on a set of open-source tools to query, validate, and analyze domain vulnerabilities. The query function searches multiple vulnerability databases using a comprehensive list of keywords relevant to the maritime domain. These vulnerabilities are then used to evaluate the overall risk picture and deduce the MITRE ATT&CK tactics and techniques. This process aims to thoroughly address maritime vulnerabilities to accurately depict the threat landscape by eliminating false positives (vulnerabilities detected based on irrelevant string matching). The findings are then summarized to capture the state of cyber vulnerabilities in the domain. The contributions of this paper can be summarized as follows:

- A tool-supported semi-automated vulnerability and threat analysis approach, reflecting the cyber risk landscape in the maritime domain based on existing known vulnerabilities (CVEs).
- Identification of the current cyber threat landscape through the application of this approach.

2 Background

2.1 Maritime Cyber Risks

The maritime infrastructure relies on various Information Technology (IT) and Operational Technology (OT) systems, including the Automatic Identification System (AIS), Electronic Chart Display and Information System (ECDIS), Global Positioning System (GPS), and Operational Technology (OT) Systems. **AIS**, mandated by the International Maritime Organization (IMO), facilitates the exchange of critical voyage information but is vulnerable to attacks due to its unauthenticated and unencrypted radio-based protocol [12,14,16,31]. **ECDIS**, essential for electronic navigation, is susceptible to attacks, especially when running outdated software, which can extend to other connected systems [10,43,44,46]. **GPS**, critical for navigation, is prone to spoofing and jamming attacks, posing operational risks [10]. **OT systems** in modern ships, when integrated with IT systems, expose isolated vulnerabilities to potential exploitation [5,10], raising concerns about potential manipulation of a ship's course or causing collisions.

Furthermore, these systems rely on specific protocols and standards used in maritime operations, such as the National Marine Electronics Association (NMEA) standard and the AIS protocol. The NMEA standard facilitates communication between marine systems by transmitting sensor data through a message-based protocol [40]. AIS, which is based on the NMEA standard, is a specialized message-based protocol that is used in various maritime services including traffic management, search and rescue, and collision avoidance [28].

The majority of academic work related to maritime cybersecurity focuses on a small subset of the domain's systems with AIS, ECIDS, and GPS as the most commonly highlighted. Therefore, broadening the research to include other maritime assets is necessary.

2.2 Threats and Vulnerability Constructs

A wide range of constructs (i.e. terminologies) exist in the cybersecurity domain to communicate aspects related to risks associated with threats and vulnerabilities. This section highlights constructs relevant to this paper, chosen based on their commonality in the literature. Definitions of each construct with examples are provided below.

- **CVE** [36] stands for Common Vulnerabilities and Exposures (e.g. CVE-2023-36857). Cybersecurity vulnerabilities are assigned entries, each including an ID number, a description, and at least one public reference.
- **CPE** [35] stands for Common Platform Enumeration. A nomenclature dictionary is commonly utilized to refer to specific hardware, operating systems, and applications. A CPE refers to a particular product, its vendor, version, and update. CVEs are usually assigned to one or several CPEs. An example is: cpe:2.3:h:bakerhughes:bentley_nevada_3500_system:-:*:*:*:*:*:*:*
- **TTP** [38] stands for Tactics, Techniques, and Procedures which are commonly utilized constructs adopted by the MITRE ATT&CK framework. Tactics refer to adversarial objectives (e.g. "TA0001: Initial Access"). Techniques refer to methods adversaries employ to achieve their objectives (e.g. "T1133: External Remote Services"). Procedures refer to the actual implementation (e.g. malware) employed to realize the adversarial technique (e.g. "S1060: Mafalda").
- **CAPEC** [34] stands for Common Attack Pattern Enumeration and Classification (e.g. CAPEC-555: Remote Services with Stolen Credentials). CAPEC provides a classification for the known attack patterns employed by attackers to exploit known weaknesses in cyber systems. Hence, by definition, it is clear that CAPECs are connected to CWEs.
- **CWE** [37] stands for Common Weakness Enumeration (e.g. CWE-522: Insufficiently Protected Credentials). CWEs are a way of categorizing the underlying weakness that caused the vulnerability (or CVE). Hence, CWEs are linked to one or more CVEs.
- **KEV** [19] standing for Known Exploited Vulnerabilities, is a list of CVEs that have been successfully exploited (e.g. CVE-2024-24919).
- **CVSS** [22] The Common Vulnerability Scoring System is a standard used to assess the severity of a CVE. It helps capture the characteristics of a vulnerability to calculate its severity score. For example, the CVSS score of CVE-2023-36857 is 6.5 (Medium). Not all CVEs have all versions of CVSS available, so this paper uses the latest version for each CVE in the analysis.
- **EPSS** [23] stands for Exploit Prediction Scoring System. It provides a way to assess the likelihood of a vulnerability being exploited. The score gives a numerical value indicating the likelihood of an exploitation attempt of a specific CVE in the next 30 days. For example, the EPSS Score of CVE-2022-3569 is 7.8 (High).

2.3 Open-source tools

We have employed two open-source tools for the development of threat exploration methodology in this paper, namely, *CVEMap*, and *BRON*.

CVEMap is an open-source command-line utility which provides a structured and easy way to navigate public CVE sources [2]. The tool uses data from various public sources giving a wide coverage of all reported vulnerabilities. The most important are the National Vulnerability Database (NVD) [39] from NIST and the CISA KEV database. Furthermore, it combines data from other sources such as Hackerone and publicly available exploits from Github. Furthermore, *CVEMap* provides capabilities to search for vulnerabilities by querying the CVE data or by vendor.

BRON [21] is a bi-directional data graph that links different threat constructs, namely, ATT&CK TTP, CWE, CVE, and CAPEC [26]. The CVE records are linked to CWEs, the CWEs are linked to CAPECs, and CAPECs are linked to ATT&CK techniques. These mappings provided by *BRON* for the different threat constructs and the ability to navigate the knowledge graph enable further exploration of the risk picture delineated by the identified CVEs to generate useful insights.

3 Related Work

3.1 Maritime Threat Landscape

The maritime cyber risk picture or what could be referred to as the threat landscape has been captured in the literature through different perspectives, including, incidents (i.e. what has happened) or threats (i.e. what may happen).

The incident perspective provides tangible intelligence and information that can be used to learn lessons to avoid repeating mistakes. Meland et al [33] captured the threat landscape in the domain by analyzing 46 maritime cybersecurity incidents between 2010-2020. The objectives of their analysis were to understand the types of threats (e.g. misuse of AIS and positioning data) facing the industry and infer the attack points (e.g. GNSS) and techniques (e.g. social engineering) to inform defences.

On the other hand, the threat perspective provides information about what may happen based on theoretical analysis or empirical evidence. Androjna et al [13] conducted a literature review to capture the cyber trends and challenges from different perspectives including attack types, surface, and impacts. The authors identified a wide range of methods threatening the shipping industry including, among others, ransomware, defamation, and digital piracy. Moreover, Amro and Gkioulos [12] conducted a literature review to capture the threat landscape in the maritime domain based on the observed tactics (i.e. objectives) and techniques (i.e. methods) utilized the MITRE ATT&CK framework [42].

3.2 Vulnerabilities and CVEs in the domain

Some works in the literature have discussed vulnerabilities in the domain without referring to specific CVEs. Svilicic et al [45] conducted a vulnerability scan and risk analysis of a ship ECDIS using the Nessus scanner. The authors identified a group of vulnerabilities mostly related to the operating system of the ECDIS. Additionally, Bothur et al [15] focused on theoretical vulnerability analysis of some ship systems such as Industrial Control Systems (ICS), AIS, and VSAT.

Other literature has discussed specific CVEs in different ways. Amro [11] identified five CVEs related to six marine devices (e.g. GPS) found to be emitting NMEA messages on the Internet. The author relied on vendor-specific messages found using the Shodan scanner to identify the device names and then utilized the NVD to discover their associated CVEs. Bronk and Dewitte [17] referred to a specific CVE in Navis software for railcar hub assignment and train load sequence planning to highlight the challenge in port security in contracts to ship security by having many more points of entry to the interconnected port systems. Hopcraft et al [27] discussed a specific CVE in VDR software to argue about the existence of unsecured devices in the world fleet. Freire et al [24] discussed an attack model that can threaten Maritime Monitoring Systems. Among the attacker's capabilities is exploring existing vulnerabilities such as PostgreSQL CVE. Grigoriadis et al [25] proposed a risk assessment framework targeted for the maritime sector. The framework utilizes the CAPEC attack patterns to describe cyber threats against assets. The framework then uses the CVSS metrics of the CVEs associated with those threats to measure the risk level. The authors demonstrated their approach by discussing the risk in eight situations (e.g. cargo loading & unloading). The risk assessment included 7 different assets across the situations with 7 unique CVEs. Juvonen et al [29] discussed the CVEs associated with Apache Log4j2 exploitation within aeronautical, maritime, and aerospace communication environments. The authors demonstrated proof of concepts for exploiting those vulnerabilities over mission-critical wireless communication protocols like ACARS, ADS-B, and AIS. Martinie et al [32] and Kalogeraki et al [30] applied the supply chain risk assessment methodology (MITIGATE) [41] to assess risks related to cargo manifest files, Maritime Logistics and Supply Chain (MLoSC) respectively. MITIGATE utilizes knowledge obtained from CVEs, CPEs, and CWEs for analyzing threats, vulnerabilities, and their impact. Martinie et al [32] referred to 6 unique CVEs to demonstrate the knowledge obtained from utilizing CVEs and CWEs for risk assessment while Kalogeraki et al [30] referenced two CVEs as examples demonstrating their proposed approach. Enoch et al [20] applied the knowledge of known vulnerabilities for assessing the risks against maritime systems based on the CVSS metrics of their associated CVEs. They demonstrated their work through 8 CVEs identified in 6 systems (e.g. Engine control system and ECDIS).

In summary, the identified works referring to CVEs in the maritime domain or applying them in different cybersecurity functions only highlight a small subset of CVEs not representative of the range of vulnerabilities in the domain. To the best of our knowledge, this paper provides the most comprehensive view of vulnerabilities in the maritime domain in addition to a semi-automated approach allowing continuous monitoring of the domain's vulnerability landscape.

3.3 Examples of Threat assessment reports

Norwegian Maritime Cyber Resilience Center (NORMA Cyber) is a hub for cybersecurity in the Norwegian maritime sector [1]. NORMA offers several services to its members, including threat intelligence, by sharing vulnerability information and mitigation advice. It also publishes threat reports every year, reviewing the cybersecurity situation of the past year based on reported incidents, vulnerabilities, etc, and forecasting an assessment for the next year. They also emphasize the importance of vulnerability information for accurate threat assessment in the annual threat assessment report.

The European Union Agency for Cybersecurity (ENISA) [3] also, in its annual threat landscape for 2023, emphasizes the importance of vulnerability information to learn about the trends in cybersecurity. The ENISA threat report uses various metrics related to vulnerabilities like CVSS score, CWEs, and KEV values.

Our tool can automatically gather information about various metrics and generate insights similar to those found in ENISA and NORMA Cyber Threat Reports. Additionally, the tool's scope can be customized based on the input keywords provided for vulnerability searches. This tool is helpful as it automates the provision of vulnerability information. It also links vulnerabilities to products, weaknesses, and attack techniques, providing organizations with a comprehensive understanding of the risk picture. Furthermore, our unique methodology covers a wide range of devices used in the maritime domain by searching for all approved device vendors in the marine industry.

4 Maritime Threat Explorer (*MaThreX*)

4.1 The *MaThreX* Process

In this section, we present the *MaThreX* methodology complete pipeline showing its application in the threat analysis of the maritime domain.

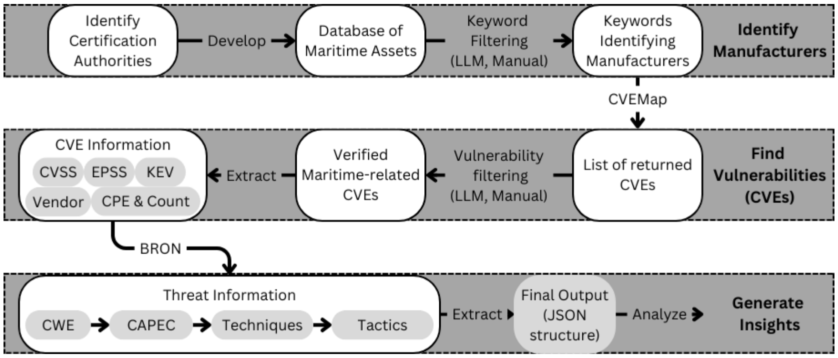
Identify Certification Authorities
Develop
Database of Maritime Assets
Keyword Filtering (LLM, Manual)
Keywords Identifying Manufacturers
Identify Manufacturers
CVEMap
CVE Information
CVSS
EPSS
KEV
Vendor
CPE & Count
Extract
Verified Maritime-related CVEs
Vulnerability filtering (LLM, Manual)
List of returned CVEs
Find Vulnerabilities (CVEs)
BRON
Threat Information
CWE
CAPEC
Techniques
Tactics
Extract
Final Output (JSON structure)
Analyze
Generate Insights

Fig. 1: The flow diagram of the *MaThreX* methodology

As shown in Figure 1, the methodology be divided into three main stages, namely, 1) listing all maritime equipment manufacturers, 2) finding the known vulnerabilities in the devices manufactured by them, and 3) compiling further information from *CVEMap* and *BRON* data to present insights about the state of maritime cybersecurity. The first stage starts by identifying maritime certification authorities to find databases of maritime equipment. These databases are then filtered to get a searchable keyword list containing maritime equipment manufacturers. The keyword list is passed to *CVEMap* in stage 2 to search for CVEs related to those manufacturers. Upon filtering the CVE list and extracting their information (e.g. CVSS, CPEs), the CVE list is input into the *BRON* tool to extract further information (e.g. CWE, CAPEC) in stage 3. Finally, all the gathered information is compiled into a final output to be analyzed to describe the state of maritime cybersecurity. The keyword and CVE filtering in stages 1 and 2 have been conducted both manually and using Large Language Models (LLM) to evaluate the utility of Artificial Intelligence (AI) in automating this process to facilitate its continuity. In the following subsections, these steps are explained in detail.

Stage 1 - Identify Manufacturers: The manufacturers were identified to compile a list of keywords to be used for searching for known vulnerabilities in the devices and equipment used in the maritime industry.

A novel approach was devised that goes top-down starting with the certification authorities that certify equipment used in the maritime infrastructure (e.g. ships) and then searching for any publicly available database of certified equipment. This led us to DNV (Det Norske Veritas) which serves as a certifying body to assess the equipment used onboard vessels and in other sectors and maintains a list of all certified devices on its approvals website [1]. *Approval Finder* by DNV is a web tool to search and verify the products, manufacturers, and service suppliers approved by DNV. On this site, one can find the certificate number, product name, expiry date, company name, country, city, and approval group of any approved entity. The website has 74,028 products listed in the database at the time of this writing. Out of these, only 41,217 have active certificates. In this paper, the devices with active certificates were considered as those with expired certificates have less chance of being actively used in ships.

Another identified certification body was the European Maritime Safety Agency (EMSA). EMSA has a list of Marine Equipment Directive (MED) applicable to ships flying the flag of an EU country, Norway or Iceland. EMSA provides a portal that keeps the list of MED-approved devices [2]. Hence, this is the most comprehensive list covering the whole EU. This database lists 190,181 different equipment used on ships, along with other information, including the company name and product type. We also found a third database from the Maritime and Coastguard Agency of the UK that contains a list of devices that are approved by the UK [3]. This is rather small compared to the previous database and contains only 2198 entries.

[1] https://approvalfinder.dnv.com/

[2] https://portal.med.emsa.europa.eu/

[3] https://www.gov.uk/government/publications/uk-marine-equipment-approval-database

In our testing, we found that using product names to search for vulnerabilities in databases may not yield accurate results. Although it may seem like using product names could reduce false positives, the way products are listed in the databases is not standardized and does not align with the vulnerability search tool. We experimented using *CVEMap* to query CVEs for a small subset of devices made by Furuno, a known maritime equipment manufacturer. The list of devices contained comma-separated models, so we separated these devices to increase the chances of finding vulnerabilities. We compiled a list of 107 keywords by taking the 'Product name' field from all entries containing the word 'Furuno' in the 'Company' column and removing duplicates. Unfortunately, the results did not yield any CVEs. However, when we searched using the company name, we found six vulnerabilities. Hence, keeping in view the discussion above and the results from the preliminary experiment, we decided to proceed with the company names as keywords for the vulnerability search.

In the filtering step, the list of companies is extracted from the databases, and the final keywords list is prepared to be fed into *CVEMap*. First, a preliminary list of companies was manually extracted from each of the three database files using Microsoft Excel. Since the DNV database also stored product categories and product types, this was done by filtering the Excel file based on the product category 'Instrumentation and Automation'. Since we are only interested in devices with cybersecurity vulnerabilities, this category was selected because it contained such devices, e.g. control systems, AIS transceivers, and ECDIS. Furthermore, it was ensured that other categories are irrelevant, e.g. machinery equipment, life-saving equipment, etc. Still, other categories that might be relevant to certain organizations might be easily added to generate the final list of manufacturers.

It is noteworthy to mention that the EU MED database did not provide product categories like DNV. Hence, a different approach based on Excel was used to filter out unwanted products like paints, winches, sewage, etc. This approach was used to remove unwanted equipment while also ensuring that relevant devices are not removed. This resulted in a reduction of products from 190181 to 69214 yielding **3175 unique companies**. This process greatly reduced the search keywords, but the companies' lists need more processing before they can be fed to *CVEMap*. The DNV company list contained many duplicates, e.g. there were 34 variants of the company ABB like ABB AG, ABB AS, ABB Automation, etc. Furthermore, the existence of characters like AS or Gmbh; abbreviations denoting the company liability type, next to company names hinders the search of companies by making it more restrictive. Also, we must be careful in removing keywords that are expected to give many hits, resulting in many false positives, because by removing useful keywords for fear of getting many false positives, we also risk ignoring keywords that would give relevant vulnerabilities too.

During the filtering step, two approaches were considered: a manual approach and an automated LLM-based approach. The manual approach includes analyzing each entry in the complete list (3889 keywords), and based on personal judgment derived from working with search terms, cleaning the list by removing keywords, removing characters, dividing the company name into multiple, making variations of the company name or remove duplicates that are expected to give the same result. On the other hand, when implementing the LLM-based approach, cleaning the keywords list was conducted by employing the GPT-4 model, the latest in the series of Generative Pre-trained Transformer models [9].

Finally, we only considered the keywords from UK MED and DNV databases because they gave a stable list covering a large set of relevant companies. However, the EU MED database list of keywords did not produce a high-quality output. It was found through smoke testing that some very famous companies were not present, and further, due to lack of product category in the data, many irrelevant companies were also present in the list.

Stage 2: Find Vulnerabilities Once we have the list of equipment manufacturers, the next step is to look for known vulnerabilities in their devices using *CVEMap*.

CVEMap provides multiple ways to look for vulnerabilities. Since we have a list of product vendors as our input, we could have done it in two ways, by querying in the CVE data or by searching through the vendor. The list of equipment could be used to search directly for products but it becomes too restrictive, and the product name in *CVEMap* and our list can vary (e.g. Furuno in our list and Furunosystems in the CVE data) hence there is a good chance that we miss out on a lot of CVEs. So, we instead went for the querying function. This also has a negative point in that it gives many false positives that need to be filtered afterwards which we are going to discuss further on.

As mentioned before, the query-based search through *CVEMap* can result in many false positives. For example, searching for a maritime-related keyword "sonar" gives CVEs related to Jenkins[4] which is an open-source automation tool used in software development and not related to any marine sonar equipment. The false match is due the SonarQube platform for code inspection integrated within Jenkins. Also, our list contains some companies like Siemens, ABB, etc, that manufacture various kinds of IT systems, including those that may not be used in maritime.

Hence, to remove these kinds of CVEs from our list, we employed manual filtering and again decided to test LLM-based filtering. GPT-4 model was employed and given CVE name and its description and asked to return a 'yes' or 'no' based on whether it could be used in a maritime setting or not.

Stage 3: Generate Insights In this step, set up our instance of the *BRON* tool on a server. The data graph is implemented in a database using ArangoDB, a graph database system. Next, we had to write our scripts to query and traverse the data graph in an automated manner using the list of CVEs. The script output is a JSON file containing arrays of CVEs containing all information found through *BRON* and other important CVE-related data used for analysis. The different fields in the final JSON structure are described in Table 1.

[4] `https://www.jenkins.io/`

Table 1: Fields in the JSON structure

Field	Description
cveId	The root object that contains details about the CVE
sourceQuery	A string storing the search term used to identify this CVE entry in *CVEMap*
countCPE	An integer representing the number of CPE entries associated with this CVE.
manufacturer	A string indicating the manufacturer or vendor of the product that has the vulnerability in the NVD database
CVSS	A floating-point number representing the CVSS score.
EPSS	A floating-point number representing the EPSS score.
KEV	A boolean indicating whether the CVE is part of the KEV catalogue
cwes	An array of strings representing CWE identifier associated with the vulnerability
capecs	An array of strings listing CAPEC identifiers associated with the vulnerability
techniques	An array of strings listing ATT&CK techniques used to exploit the vulnerability
tactics	An array of strings listing ATT&CK tactics associated with the techniques

Finally, the output JSON structure can be used for visualizing and analyzing the wide range of information extracted from the *MaThreX* tool. Microsoft Power BI [5] is merely an example and it was employed in this paper. Power BI was chosen for its robust visualization capabilities, allowing the creation of interactive and insightful dashboards and reports. With Power BI, it was possible to visually represent various aspects of the data, including trends, patterns, and correlations, thereby facilitating a comprehensive analysis of the information gathered from the tool.

4.2 *MaThreX* results

In this section, we will describe the results obtained by running the *MaThreX* tool against the DNV and UK MED databases. The final vendor list comprised 803 keywords (691 from DNV, 143 from UK MED, and 31 commons). Out of which, 52 gave hits in *CVEMap*, resulting in 928 CVEs. Upon removing duplicates and false positives, 27 keywords and 244 CVEs remained. The next step is to dive deeper into the CVEs and identify details about the vulnerabilities. This involved querying the *BRON* database to identify CPEs, CWEs, CAPECs, Techniques, and Tactics for each vulnerability. Table 2 shows the final number of these threat constructs found during our research. In the following subsections, we will correlate the different constructs related to the CVEs found in maritime assets to gain deep insights into the maritime threat landscape. All the results including the final list of vendors and vulnerabilities (with false positives and filtered) are provided in our online repository [6].

Table 2: Summary of the threat constructs generated by *MaThreX*

Threat construct	CVEs	CPEs	CWEs	CAPECs	Techniques	Tactics
Count	244	1810	94	391	234	14

[5] https://app.powerbi.com/

[6] https://github.com/ahmed-amro/MaThreX

Trend over the years Figure 2 plots the number of CVEs by year. The plot shows an overall increase in reported vulnerabilities over the years, with the number of CVEs peaking in the year 2023 with 93 vulnerabilities. This healthy trend indicates an increase in scanning for vulnerabilities in these systems.

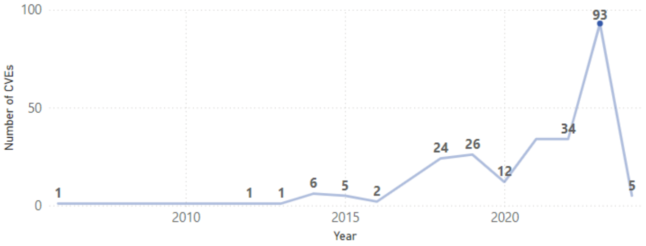

Fig. 2: Reported Vulnerabilities Trend over the years

Severity & Exploitability Severity and Exploitability combined can help decision-makers prioritize the vulnerabilities that need to be fixed urgently. Figure 3 shows the severity by plotting the CVSS scores of the identified vulnerabilities. Since the CVSS score ranges between 1-10, the scores are divided into bins for this visualization. The figure shows a slight tilt towards the higher CVSS scores, with the topmost bin of CVSS scores 8.9-9.45 having 38 CVEs. Most CVEs (53) lie between the range of 6.7-7.25. This shows that the CVEs affecting the maritime systems are mostly of higher severity.

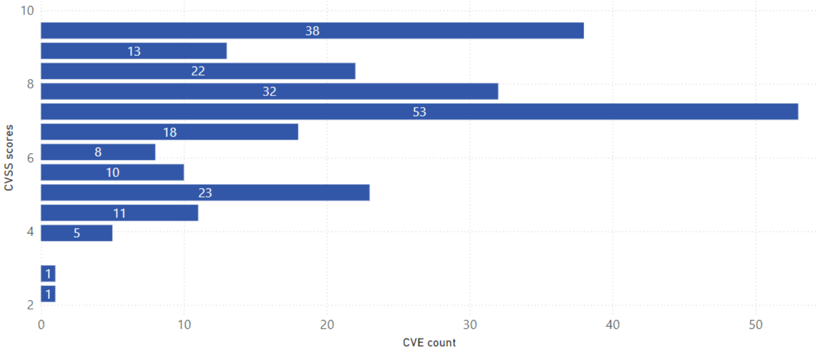

Fig. 3: CVSS scores of identified vulnerabilities

Regarding the EPSS scores, which reflect the exploitability or likelihood of vulnerabilities being exploitable in the near future. Almost all of the vulnerabilities have a very low value of <0.04, which is expected since no vulnerability was found to be listed in the KEV catalogue as known exploitable CVEs. There is only one outlier with a score of 0.84 for a CVE assigned to Wago. This is a positive indicator regarding the reduced exploitability of maritime vulnerabilities with few exceptions. Still, this metric changes frequently based on the availability of exploits to the found vulnerabilities. This motivates frequent execution of such analysis to maintain an up-to-date threat picture.

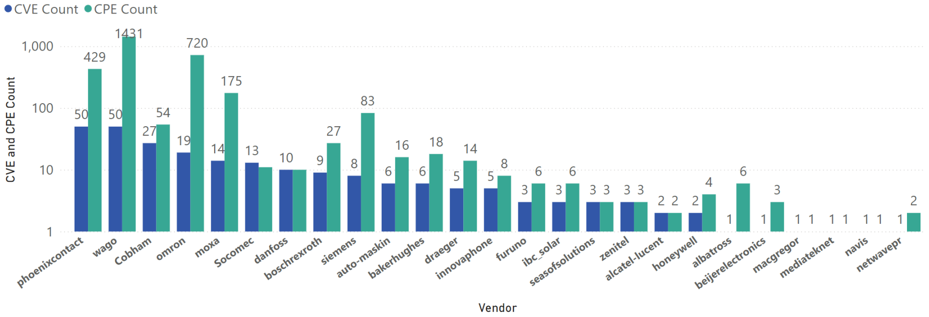

Fig. 4: Number of CVEs and CPEs by vendor on a logarithmic scale

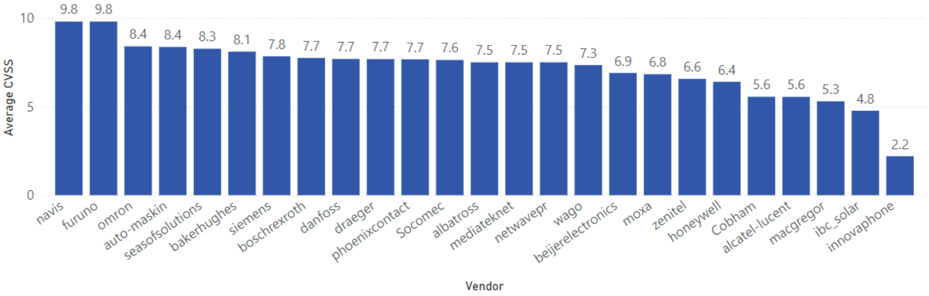

Fig. 5: Average CVSS by vendor

Insights about vendors A very important use case of CVE data and related information is the insights gathered about different vendors. This information can be helpful in several ways including supply chain management. Figure 4 shows the vendors with the most known vulnerabilities and the number of products (i.e. CPEs) affected by those vulnerabilities. Similarly, Figure 5 shows the average vendor-based CVSS score information.

Noteworthy, just seeing a single metric alone might give an incomplete picture. As shown in Figure 4, Phoenix Contact has the most identified vulnerabilities (along with Wago). However, it is the third regarding the number of product versions affected by these vulnerabilities. Another insight appears when considering the number of CVEs and the average CVSS scores. For example, Navis has only a single reported vulnerability for a single CPE as shown in Figure 4 while this vulnerability has the highest CVSS score as shown in Figure 5.

Weaknesses and Adversaries related insights Table 3 shows the top 10 most occurring weaknesses related to the identified CVEs including their description. The finding of CWE-798 weakness as the top weakness emphasizes the threats posed by the use of hardcoded credentials in maritime equipment. This is a very important insight as it provides actionable information to vendors and users of the equipment to focus on weaknesses to make them secure.

Table 3: Top 10 CWEs

ID	CVE Count	(%)	Description
798	19	13.77%	Use of Hard-coded Credentials
79	18	13.04%	Improper Neutralization of Input During Web Page Generation
78	15	10.87%	Improper Neutralization of Special Elements in an OS Command
200	14	10.14%	Exposure of Sensitive Information to an Unauthorized Actor
306	14	10.14%	Missing Authentication for Critical Function
787	12	8.7%	Out-of-bounds Write
80	9	6.52%	Improper Neutralization of Script-Related HTML Tags in a Web Page
20	8	5.8%	Improper Input Validation
732	8	5.8%	Incorrect Permission Assignment for Critical Resource
287	7	5.07%	Improper Authentication

Furthermore, the top 10 CAPEC patterns, ATT&CK techniques, and tactics are presented in Tables 4, Table 5, and Table 6 respectively. These metrics provide key insights into the methods adversaries may use to compromise systems. The information was retrieved by navigating the *BRON* data graph.

Table 4: Top 10 CAPEC IDs

ID	CVE Count	(%)	Description
60	9	5.45%	Reusing Session IDs (aka Session Replay)
22	8	4.85%	Exploiting Trust in Client
55	8	4.85%	Rainbow Table Password Cracking
59	8	4.85%	Session Credential Falsification through Prediction
122	7	4.24%	Privilege Abuse
26	7	4.24%	Leveraging Race Conditions
76	7	4.24%	Manipulating Web Input to File System Calls
79	7	4.24%	Using Slashes in Alternate Encoding
102	6	3.64%	Session Sidejacking
20	6	3.64%	Encryption Brute Forcing

As an example, the attack pattern with the highest CVE count is CAPEC-60: Reusing Session IDs (aka Session Replay). Coupled with this, the most often employed technique is T1027.009, which involves the use of obfuscated files or information, specifically through embedded payloads. This attack pattern and technique align with the most prevalent ATT&CK tactics Defense Evasion (TA0005). These metrics together provide a comprehensive understanding that allows for improved threat modelling, vulnerability management, and the implementation of targeted security measures to defend against real-world threats.

Table 5: Top 10 ATT&CK Techniques

Techniques	CVE Count	(%)	Description
T1027.009	14	7.14%	Obfuscated Files or Information: Embedded Payloads
T1040	10	5.10%	Network Sniffing
T1134.001	10	5.10%	Token Impersonation/Theft
T1499.002	10	5.10%	Endpoint Denial of Service: Service Exhaustion Flood
T1539	10	5.10%	Steal Web Session Cookie
T1110.002	9	4.59%	Brute Force: Password Cracking
T1110.003	9	4.59%	Brute Force: Password Spraying
T1550.004	9	4.59%	Use Alternate Authentication Material: Web Session Cookie
T1558.003	9	4.59%	Steal or Forge Kerberos Tickets: Kerberoasting
T1005	8	4.08%	Data from Local System

Table 6: Top 10 ATT&CK Tactics

Tactic	CVE Count	(%)	Description
TA0005	56	12.47%	Defense Evasion
TA0003	52	11.58%	Persistence
TA0006	52	11.58%	Credential Access
TA0004	46	10.24%	Privilege Escalation
TA0007	38	8.46%	Discovery
TA0009	36	8.02%	Collection
TA0001	35	7.80%	Initial Access
TA0040	32	7.13%	Impact
TA0008	29	6.46%	Lateral Movement
TA0011	21	4.68%	Command and Control

4.3 Comparing Manual and LLM-based filtering

During the testing of keyword filtering, we used an LLM method with a list of companies from DNV to obtain CVEs and then compared the results with a manual list. The LLM method, although effective in many cases and covering numerous results, was not as effective as manual filtering. It missed some useful keywords, and the keyword-cleaning process was not very effective in some cases. Therefore, we do not recommend it as an effective method for filtering keywords, as skipping important CVEs at this crucial step will lead to an incomplete threat assessment. Additionally, the effort required for manual filtering is manageable in this case and is not needed so frequently when creating a list of manufacturers.

For CVE filtering, we passed the list of CVEs obtained from *CVEMap* to GPT-4 to filter only maritime-related CVEs. We provided 852 CVEs, along with their descriptions, to the model, which is less than the actual list of CVEs obtained from *CVEMap* (928 CVEs). This is because the list from *CVEMap* contains some duplicate CVEs in cases where two keywords returned the same CVE. Additionally, it was not possible to obtain descriptions for some CVEs with their status listed as 'awaiting analysis'.

The results of the filtering were not very promising. The model returned 'Yes' for 56 and 'No' for 796 CVEs. Upon comparing the CVEs with the list obtained from manual filtering, considered as the ground truth, it was found that the tool correctly identified 35 out of 56 as maritime-related CVEs, while the remaining 21 were incorrectly characterized as such. Similarly, 592 CVEs were correctly classified, while 204 were incorrectly classified as unrelated to the maritime industry. This resulted in an accuracy of 73.6%.

Ideally, the accuracy should be higher. These results suggest that the model can somewhat reason about the CVEs. However, due to the reduced accuracy, the model is insufficient for practical application. Consequently, these results indicate that the current implementation of LLM models is unsuitable for our application. Therefore, based on the available LLM models, this paper suggests a manual approach. However, the model might be improved by providing more training data or context.

5 Discussion

5.1 Maritime Threat Landscape

The *MaThreX* methodology gathers data on vulnerabilities in the maritime industry to understand its cybersecurity state. This is the first work of its kind for this sector. By examining vulnerabilities, we can describe threats based on empirical evidence and understand attackers' abilities. In this section, we examine the threat landscape from the perspectives of adversarial tactics and techniques, and attack patterns. These perspectives are derived from threat-related information associated with discovered vulnerabilities.

We can infer the adversarial objectives the vulnerabilities can support by looking at the ATT&CK tactics. The results suggest that the vulnerabilities can support all 14 enterprise tactics from reconnaissance to impact. We can also infer the methods the attackers can apply to exploit the vulnerabilities by looking at the ATT&CK techniques. The results suggest that the vulnerabilities can support 234 techniques which constitute about 54% of the entire ATT&CK enterprise techniques. Considering the range of both tactics and techniques, attackers have flexibility in developing a variety of multi-stage attacks (i.e. kill chains) within the maritime assets.

We can also infer the attack patterns that adversaries can employ to exploit the vulnerabilities by looking at the CAPEC patterns. The vulnerabilities can be exploited through 391 CAPEC patterns which constitute about 70% of the entire CAPEC list. However, the distribution of patterns relevant to each vulnerability is flat, meaning that 73% of attack patterns can exploit 1 or 2 vulnerabilities.

On the other hand, only 27 patterns enable the exploitation of 5 or more vulnerabilities. Those patterns (partially shown in Table 4) can be considered to constitute a higher risk and would be logical to be prioritized for mitigations.

Lastly, this methodology can also be applied to other industries (e.g. energy) or organizational levels to capture the threat landscape by adjusting the keyword list to control the scope of target assets.

5.2 Limitations

Although the *MaThreX* methodology generates robust results and insightful findings, some limitations must be mentioned to further improve the process in the future. Starting with the dataset issues such as including missing product types and categories, incorrect types or categories, and inconsistencies in company naming conventions. These inconsistencies can affect the accuracy and reliability of the tool. Addressing these issues by refining and standardizing the data sources will significantly enhance the tool's performance and the validity of its findings.

Another issue is the manual filtering of keywords and CVEs which can be considered subjective. Different considerations were made while cleaning the companies' keywords list. The addition of a keyword giving false hits does not affect the output of the tool but only makes the next stage which filtering the CVEs harder. However, if a useful keyword is ignored for the fear of getting too many false positives, then as a result, the tool can skip important vulnerabilities. However, it is equally important to be careful while adding or removing CVEs in the next stage because having unrelated vulnerabilities in the final list will skew our view of the state of maritime cybersecurity.

Lastly, in the results section, we have shown the tool's potential by picking some interesting comparisons from the data. For example, the section related to vendors shows how this tool can help make informed decisions while selecting a vendor based on their cybersecurity posture. Similarly, CWEs, CAPECs, and MITRE Tactics and Techniques provide insights into attackers' behaviour. We believe that there can be a lot more interesting comparisons made through this data based on the use case.

6 Conclusions

This research focuses on analyzing vulnerabilities and threats within maritime systems. By analyzing 244 maritime-related vulnerabilities identified by 803 keywords comprising maritime equipment manufacturers, this study provides a detailed understanding of the state of maritime cybersecurity. The identified CVEs affect 1810 CPEs (or product versions). The trend showing an increase in reported vulnerabilities and insights like those about maritime vendors is key in reflecting the state of maritime cybersecurity from the perspective of the reported vulnerabilities. Additionally, the threat of hardcoded credentials has been confirmed in this study as the highest occurring weakness enabling the discovered vulnerabilities. Furthermore, our analysis suggests that the vulnerabilities can enable a range of kill chains due to their association with a large number of tactics, techniques and attack patterns.

Some improvements can be made regarding the *MaThreX* tool. By incorporating more databases into the input, we can improve the coverage of the tool. Furthermore, the tool can be converted to a complete automated analysis framework by incorporating AI or customized LLM-based solutions to replace the manual work related to keyword filtering and CVE filtering. Specialized LLM-based solutions can also be applied in the final step to generate insights from the gathered data. The methodology must also be rigorously tested in different case studies to empirically assess its utility.

In summary, this study provides a method for continuous understanding of the threat landscape in maritime systems, highlighting the potential and limitations of the proposed method for future advancements in maritime cybersecurity. Safeguarding the security and resilience of maritime assets is crucial, and continued research and development will be vital for protecting these critical infrastructures from sophisticated cyber threats.

References

1. Annual threat assessment 2024 — norma cyber. `https://www.normacyber.no/news/annual-threat-assessment-2024`, (Accessed on 04/21/2024)
2. cvemap overview - projectdiscovery documentation. `https://docs.projectdiscovery.io/tools/cvemap/overview`, (Accessed on 04/29/2024)
3. Enisa. `https://www.enisa.europa.eu/`, (Accessed on 04/22/2024)
4. Guidelines on maritime cyber risk management. `http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC.1-CIRC.1526(E).pdf`
5. Maritime cyber security: A comprehensive approach. `https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach`, (Accessed on 12/07/2023)
6. Ur e26 rev1 cr - cyber resilience of ships. `https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/02/04140503/UR-E26-Rev.1-Nov-2023-CR.pdf`, accessed: 21.03.2024
7. Ur e27 rev cln - cyber resilience of on-board systems and equipment. `https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103853/UR-E27-Rev.1-Sep-2023-CLN.pdf`, accessed: 21.03.2024
8. Global industry report: The great disconnect. `https://cyberowl.io/resources/global-maritime-industry-report-the-great-disconnect/` (2022), accessed: 21.03.2024
9. Achiam, J., Adler, S., Agarwal, S., Ahmad, L., Akkaya, I., Aleman, F.L., Almeida, D., Altenschmidt, J., Altman, S., Anadkat, S., et al.: Gpt-4 technical report. arXiv preprint arXiv:2303.08774 (2023)
10. Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., Michaloliakos, M.: Cybersecurity challenges in the maritime sector. Network **2**(1), 123–138 (2022)
11. Amro, A.: Cyber-physical tracking of iot devices: A maritime use case. In: Norsk IKT-konferanse for forskning og utdanning. No. 3 (2021)

12. Amro, A., Gkioulos, V.: From click to sink: Utilizing ais for command and control in maritime cyber attacks. In: European Symposium on Research in Computer Security. pp. 535–553. Springer (2022)
13. Androjna, A., Brcko, T., Pavic, I., Greidanus, H.: Assessing cyber challenges of maritime navigation. Journal of Marine Science and Engineering **8**(10), 776 (2020)
14. Balduzzi, M., Pasta, A., Wilhoit, K.: A security evaluation of ais automated identification system. In: Proceedings of the 30th annual computer security applications conference. pp. 436–445 (2014)
15. Bothur, D., Zheng, G., Valli, C.: A critical analysis of security vulnerabilities and countermeasures in a smart ship system (2017)
16. Botunac, I., Gržan, M.: Analysis of software threats to the automatic identification system. Brodogradnja: Teorija i praksa brodogradnje i pomorske tehnike **68**(1), 97–105 (2017)
17. Bronk, C., Dewitte, P.: Maritime cybersecurity: meeting threats to globalization's great conveyor. In: Cyber Security: Critical Infrastructure Protection, pp. 241–254. Springer (2022)
18. Committee, T.M.S.: International maritime organization (imo) (2017) guidelines on maritime cyber risk management. `http://bit.ly/MSC428-98` (2017)
19. Cybersecurity and Infrastructure Security Agency (CISA): Known exploited vulnerabilities catalog. `https://www.cisa.gov/known-exploited-vulnerabilities-catalog`, accessed: 2024-06-19
20. Enoch, S.Y., Lee, J.S., Kim, D.S.: Novel security models, metrics and security assessment for maritime vessel networks. Computer Networks **189**, 107934 (2021)
21. Erik Hemberg and Jonathan Kelly and Michal Shlapentokh-Rothman and Bryn Reinstadler and Katherine Xu and Nick Rutar and Una-May O'Reilly: Github page for bron - link and evaluate public threat and mitigation data for cyber hunting. `https://github.com/ALFA-group/BRON`, accessed: 2024-06-19
22. FIRST: Common vulnerability scoring system (cvss). `https://www.first.org/cvss/`, accessed: 2024-06-19
23. FIRST: Exploit prediction scoring system (epss). `https://www.first.org/epss/`, accessed: 2024-06-19
24. Freire, W.P., Melo Jr, W.S., do Nascimento, V.D., Nascimento, P.R., de Sá, A.O.: Towards a secure and scalable maritime monitoring system using blockchain and low-cost iot technology. Sensors **22**(13), 4895 (2022)
25. Grigoriadis, C., Laborde, R., Verdier, A., Kotzanikolaou, P.: An adaptive, situation-based risk assessment and security enforcement framework for the maritime sector. Sensors **22**(1), 238 (2021)
26. Hemberg, E., Kelly, J., Shlapentokh-Rothman, M., Reinstadler, B., Xu, K., Rutar, N., O'Reilly, U.M.: Linking threat tactics, techniques, and patterns with defensive weaknesses, vulnerabilities and affected platform configurations for cyber hunting. arXiv preprint arXiv:2010.00533 (2020)
27. Hopcraft, R., Harish, A.V., Tam, K., Jones, K.: Raising the standard of maritime voyage data recorder security. Journal of Marine Science and Engineering **11**(2), 267 (2023)
28. IMO: Resolution a.1106(29) revised guidelines for the onboard operational use of shipborne automatic identification systems (ais) (2015)
29. Juvonen, A., Costin, A., Turtiainen, H., Hämäläinen, T.: On apache log4j2 exploitation in aeronautical, maritime, and aerospace communication. IEEE Access **10**, 86542–86557 (2022)

30. Kalogeraki, E.M., Papastergiou, S., Mouratidis, H., Polemi, N.: A novel risk assessment methodology for scada maritime logistics environments. Applied Sciences **8**(9), 1477 (2018)
31. Levy, S., Gudes, E., Hendler, D.: A survey of security challenges in automatic identification system (ais) protocol. In: International Symposium on Cyber Security, Cryptology, and Machine Learning. pp. 411–423. Springer (2023)
32. Martinie, C., Grigoriadis, C., Kalogeraki, E.M., Kotzanikolaou, P.: Modelling human tasks to enhance threat identification in critical maritime systems. In: Proceedings of the 25th Pan-Hellenic Conference on Informatics. pp. 375–380 (2021)
33. Meland, P., Bernsmed, K., Wille, E., Rødseth, Ø., Nesheim, D.: A retrospective analysis of maritime cyber security incidents. TransNav: International Journal on Marine Navigation & Safety of Sea Transportation **15**(3) (2021)
34. MITRE: Common attack pattern enumeration and classification (capec). `https://capec.mitre.org/`, accessed: 2024-06-19
35. MITRE: Common platform enumeration (cpe). `https://cpe.mitre.org/`, accessed: 2024-06-19
36. MITRE: Common vulnerabilities and exposures (cve). `https://cve.mitre.org/`, accessed: 2024-06-19
37. MITRE: Common weakness enumeration (cwe). `https://cwe.mitre.org/`, accessed: 2024-06-19
38. MITRE: Mitre att&ck. `https://attack.mitre.org/`, accessed: 2024-06-19
39. NIST: National vulnerability database (nvd). `https://nvd.nist.gov/vuln`, accessed: 2024-06-19
40. NMEA: National marine electronics association - nmea0183 standard (2002)
41. Schauer, S., Polemi, N., Mouratidis, H.: Mitigate: a dynamic supply chain cyber risk assessment methodology. Journal of Transportation Security **12**(1), 1–35 (2019)
42. Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G., Thomas, C.B.: Mitre att&ck: Design and philosophy. Technical report (2018)
43. Svilicic, B., Brčić, D., Žuškin, S., Kalebić, D.: Raising awareness on cyber security of ecdis. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation **13**(1), 231–236 (2019)
44. Svilicic, B., Kamahara, J., Celic, J., Bolmsten, J.: Assessing ship cyber risks: A framework and case study of ecdis security. WMU Journal of Maritime Affairs **18**, 509–520 (2019)
45. Svilicic, B., Kamahara, J., Rooks, M., Yano, Y.: Maritime cyber risk management: An experimental ship assessment. The Journal of Navigation **72**(5), 1108–1120 (2019)
46. Svilicic, B., Rudan, I., Jugović, A., Zec, D.: A study on cyber security threats in a shipboard integrated navigational system. Journal of marine science and engineering **7**(10), 364 (2019)