An Open-Source Database of Cyberattacks on the Maritime Transportation System

Jeroen Pijpker , Stephen McCombie , Saul Johnson , Rob Loves , Georgios Michail Makrakis *

Posted Date: 25 October 2024

doi: 10.20944/preprints202410.1996.v1

Keywords: maritime; cybersecurity; cyber threat intelligence (CTI); maritime industry

Article

An Open-Source Database of Cyberattacks on the Maritime Transportation System

Jeroen Pijpker [1], Stephen McCombie [2], Saul Johnson [1], Rob Loves [1] and Georgios Michail Makrakis [1,*]

[1] Maritime IT Security Research Group, NHL Stenden, Emmen, The Netherlands; jeroen.pijpker@nhlstenden.com (J.P.); saul.johnson@nhlstenden.com (S.J.); rob.loves@nhlstenden.com (R.L.)
[2] Maritime IT Security Research Group, NHL Stenden, Leeuwarden, The Netherlands; stephen.mccombie@nhlstenden.com
* Correspondence: george.makrakis@nhlstenden.com

Abstract: The Global Maritime Transportation System (GMTS) is a complex system of systems, encompassing port operations, shipping lines for both cargo and passengers, manufacturing, vessel traffic control, and the vessels themselves. In recent decades, cybersecurity incidents targeting the GMTS have grown significantly in both frequency and economic impact. In response to this escalating threat, we initiated a comprehensive effort in 2021 to systematically collect and catalog all publicly known cybersecurity incidents affecting the GMTS. Drawing from peer-reviewed research, news articles, and government reports, we compiled this data into the Maritime Cyber Attack Database (MCAD). Our dataset, spanning 2001 to 2023, includes over 290 cybersecurity incidents–representing a several-fold increase from the 46 incidents reported in previous research conducted in 2020. These incidents involve 54 countries and over 50 vessels, in addition to various GMTS-associated entities such as ports. The attribution of these incidents points to a range of known nation-state and criminal threat actors. This paper presents MCAD as a novel cyber threat intelligence tool and provides a high-level analysis of the collected data, offering insights into the evolving cyber threat landscape within the GMTS.

Keywords: maritime; cybersecurity; cyber threat intelligence (CTI); maritime industry

1. Introduction

The frequency of cyberattacks against the Global Maritime Transportation System (GMTS) has increased drastically year-on-year since the turn of the millennium with a corresponding increase in their overall economic impact [1]. Notable incidents, such as the impact of NotPetya malware on Maersk [2] and the ransomware attack on the Port of Nagoya [3], underscore the severe repercussions these events have on the entire industry. Unfortunately, the maritime cybersecurity community faces key obstacles to studying this phenomenon with a view to developing countermeasures, facilitating scholarly discussion, supporting informed decision-making within organisations and enabling policymakers to work in a data-driven manner. One of the most significant of these is the difficulty researchers face in amassing sufficient data relating to maritime cybersecurity incidents to facilitate practical studies. Data for such incidents spread across scholarly literature, news articles, technical and governmental reports, and a plurality of other media [4–6]. Where such data is available, it is often as part of larger general-purpose datasets made up mostly of incidents not directly relevant to the maritime domain, and thus lacking vital maritime-specific context (e.g. GPS coordinates of the victim) even when it comes to incidents that *are* of interest to the maritime community.

This disperse and segmented nature of maritime cybersecurity incidents, hampers the efforts of researchers. Without the facility to import the datasets into their tooling of choice for further analysis, any researcher consumes a significant amount of time to manually curate and pre-process the data before the analysis step takes place. Therefore, any research artefact designed to help overcome this barrier to maritime cybersecurity research should be designed not only for the completeness of its data, but also with usability in mind.

In 2021, with the aim of helping to overcome this barrier, we began a research effort to compile data on all publicly-known maritime cybersecurity incidents into the *Maritime Cyber Attack Database*

 doi:10.20944/preprints202410.1996.v1

(MCAD)—a newly-developed user-friendly cross-platform application backed by a database of incidents conforming to MITRE's *Structured Threat Information eXpression* (STIX) format [7] for easy interoperation with other tools [8].

This research effort is well-motivated. The criticality and fragility of worldwide supply chains was thrown into sharp relief during the COVID-19 pandemic, and is particularly evident within the GMTS. As a system of systems including not just vessels but also waterways, ports, and land-side connections moving people and goods to and from the water, the role of GMTS in the global economy is significant. Over 80% of the world's cargo is transported by ship [9], representing 70% of global trade by value [10]. As cybersecurity in the context of the GMTS becomes ever more critical, fleets and the technology that comprises them are ageing, increasing their vulnerability to cyberattacks. 38% of oil tankers and 59% of general cargo ships are more than 20 years old [11].

In this work, we discuss the research and development of MCAD, and apply it in the analysis of trends in maritime cybersecurity incidents since 2001. Drawing on over 290 total incidents, with the number of incidents available for any specific analysis varying due to incomplete data for some cases, we present visualizations of global trends in the frequency of maritime cybersecurity incidents. This includes further analysis by incident type, as well as the geographical origins of both threat actors and victim organizations across 54 countries. The accompanied application features a map-like interface that allows the user to view information related to that particular incident, including the location of incidents as in Figure 1. Our collection and analysis pipeline consists of a) definition of a set criteria, b) the acquisition of data from public sources or via the self-reporting functionality of our application, c) the structure of data based on STIX, and d) the visualization of data into the interactive map and charts. MCAD is already contributing in different applications such in the creation of the *Cyber Security Workbook for On Board Ship Use* [12].

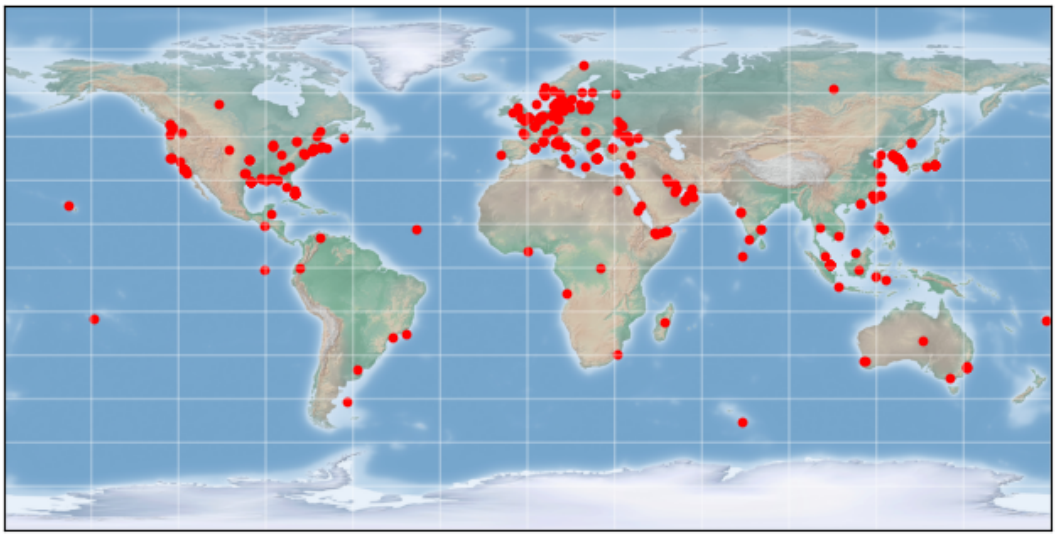

Figure 1. Incidents noted in the MCAD database at time of publication, plotted according to their geo-location on a map of the world.

While this is an open-ended research, early findings provide valuable insights into the evolving cybersecurity threats faced by the GMTS. These findings underscore the urgency for industry, government, and the research community to collaborate on improving the security posture of these critical systems.

The rest of the paper is structured as follows: In Section 2, we discuss related work appearing in the published literature. We present the methodology behind the MCAD application and assemble its underlying dataset in Section 3 while in Section 4 an evaluation and analysis of the dataset takes place. In Section 5, we acknowledge the limitations of our work and outline our plan to address them, before providing some concluding remarks in Section 6.

 doi:10.20944/preprints202410.1996.v1

2. Related Work

The work presented in this paper is not the first to create a curated open-source database of cybersecurity incidents. Such databases are fundamental to modern information security research and CTI. For example, a study by Harry and Gallagher in 2018 proposed a taxonomy for classifying cybersecurity incidents and applied this taxonomy to analyze over 2,400 cybersecurity events that occurred between 2014 and 2016. Since their publication, the *Centre for International and Security Studies at Maryland (CISSM)* has continued to curate this database, making the data publicly available for researchers. Additionally, CISSM maintains an online dashboard that allows users to explore the database and provides visualizations of key statistics. Nevertheless, their focus is more general and not specific to the in-depth analysis of maritime incidents.

In 2022, the *European Repository of Cyber Incidents (EuRepoC)* research consortium launched the *Cyber Incident Dashboard*. This initiative regularly makes its dataset available to researchers, aiming to facilitate data-driven discussions and policymaking concerning the cyber threat landscape. However, EuRepoC focuses exclusively on cybersecurity incidents with a political dimension, meaning that non-political cyberattacks—such as those targeting private organizations by cybercriminal groups for financial gain—are not included in their database.

The database most closely related to our work is the Advanced Dataset of Maritime cyber Incidents ReleAsed for Literature (ADMIRAL), which is based on the research of Olivier Jacq [16]. ADMIRAL contains 459 publicly disclosed maritime cybersecurity incidents from 1980 to 2024, categorizing them into 16 different incident types across 64 countries, impacting 22 subsectors of maritime activities. It also offers a STIX 2.1 JSON resource, which remains in an experimental phase at the time of this writing. However, ADMIRAL does not provide comprehensive information about all incidents, including references to external sources. In contrast, MCAD, offers more detailed information (as described in Section 3), enabling a thorough analysis of maritime incidents.

3. Materials & Methods

Two methods were used to compile data for MCAD. The first method involved a systematic review of scholarly literature, news feeds, technical reports and other media to identify maritime *cyber incidents*. For our purposes, we define a cyber incident as a *discrete malicious attack with a cyber element, perpetrated by a particular threat actor against one or more victims and causing significant impact on one or more victims, possibly over an extended period of time*. We consider a cyber incident eligible for inclusion in MCAD if it involves at least one component of the GMTS, which we define as a *system of systems, comprising port operations, cargo and passenger shipping lines, manufacturing, vessel traffic control, and vessels themselves*.

Our pipeline begins with defining the criteria that each collected incident must meet to be included in our dataset. These criteria are established with the unique characteristics of GMTS in mind. For example, while a cargo shipping company may be headquartered in a specific country, incidents affecting them could occur while operating abroad. As such, we identify the following essential attributes that must be present for each collected incident:

- Date - Month and Year the incident took place or it became known.
- Impact area - The GMTS are impacted, can be: Shore, Offshore, and Vessel.
- Incident Location - The location of where the incident took place.
- Incident Country - The country in which the incident took place
- GPS coordinates - Approximate latitude and longitude of the place the incident took place.
- Victim Country - The country in which the victim resides.
- Victim Identity - The name of the victim affected.
- Victim type - Type of victim related to GMTS, examples: Ship Builder, Logistics Provider, Marine Technology Provider.
- Method - The attack method used by the threat actor.
- Attacker Country - The country in which the threat actor operates from.

 doi:10.20944/preprints202410.1996.v1

These attributes are designed to enable straightforward analysis and classification of incidents, such as categorizing them by attack method, to support the creation of visualizations. As the development of MCAD is an ongoing research effort, with regular updates to the application and its database to maintain relevance and expand functionality, adherence to the established criteria gives us confidence that MCAD will become an indispensable source of CTI in the maritime domain.

Next, information for the MCAD database was gathered exclusively from public sources. This approach allows users to easily verify the legitimacy of the recorded incidents, promotes information sharing, and ensures no additional exposure of victims. The public sources used include published research, mainstream news articles, industry publications, cybersecurity vendor reports, government reports, and press releases, with references to these sources maintained as part of the corresponding MCAD entries. An illustrative but not conclusive list used to compile MCAD, based on scholarly work is presented in Table 1.

Table 1. A selection of the published scholarly work used to compile MCAD.

Year	Title	Summary	No. Attacks
2019	Maritime Cyber Security Analysis – How to Reduce Threats? [13]	Provides examples of cyber attacks against the maritime industry. Also it discusses different attacks forms that can be used and introduces different steps to mitigate cyber incidenst.	9
2020	Claims of State-Sponsored Cyberattack in the Maritime Industry [4]	Emphasizes the impact of cyber attacks on the maritime industry due to its widespread use of information technology (IT) and operational technology (OT). It also examines various cyberattacks in the maritime industry.	22
2021	A Retrospective Analysis of Maritime Cyber Security Incidents [6]	Summarizes different IT/OT attacks to the maritime industry. A total of 46 incidents are summarized between 2010 - 2020.	46
2021	A Structured Analysis of Information Security Incidents in the Maritime Sector [5]	Provides an overview about publicly known cyber incidents in the maritime sector from the past 20 years. It covers 90 publicly reported attacks and 15 proof of concepts, categorizing them into different threat categories.	90
2021	Maritime Cybersecurity: Vulnerabilities and counter measures [14]	Describes the cyber threats to the maritime industry. It discusses 9 recent cyberattacks and incidents on maritime infrastructure.	9
2022	Cybersecurity Challenges in the Maritime Sector [15]	Explores the increasing cybersecurity breaches in the maritime industry due to digitalization, highlighting vulnerabilities, consequences of cyber attacks, and mitigation actions. The paper summarizes 13 attacks against the maritime industry.	13

The second method for data input, involved the deployment of a self-report mechanism as part of the MCAD application itself, that can be seen in Figure 2. With this feature, we encourage the reporting of new incidents by users of our application. After the submission of a new entry, automatic and manual validation of the reported incidents takes place. So far, this feature of MCAD has seen a small number of uses, since submissions seldom exhibit the level of accuracy or completeness necessary for their direct inclusion in the database. We discuss potential reasons for this issue, as well as planned future work to address it, in Section 5.

 doi:10.20944/preprints202410.1996.v1

Based on the collected data, we structured the database schema after the STIX format from the MITRE Corporation, an extensible JSON-based language and serialization format used to exchange CTI. With STIX, security teams can automatically share threat information with partners or ingest it into their security systems and threat intelligence platforms. This reduces manual effort and speeds up threat detection and response. For our purposes, we augment the STIX format with the aforementioned attributes/criteria specifically related to the maritime sector.

Finally, we provide visualizations for the analysts to better understand and communicate threat intelligence findings to different stakeholders, including non-technical staff, management, or external partners. Visual formats like dashboards or charts allow for a clearer presentation of information, making it accessible to a wider audience who may not be familiar with the technical details of the analyzed incidents.

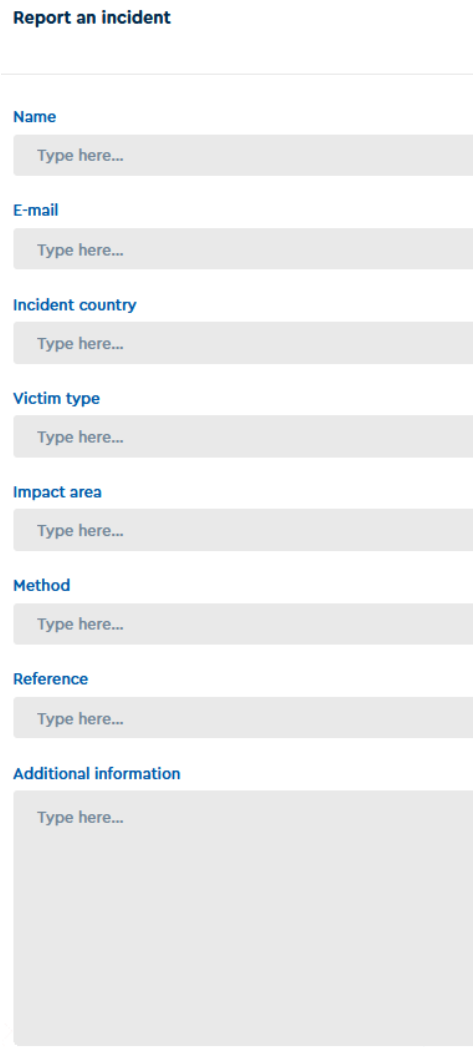

Figure 2. A screenshot of the simple user interface MCAD for the self-reporting of incidents.

4. Evaluation

We dedicate this section to an analysis of the data contained within MCAD including global trends; and incident frequencies by threat actor geography, victim geography, and attack method (e.g. ransomware, phishing). The whole database is accessible in our web app [1]. Henceforth, the number of

[1] https://maritimecybersecurity.nl.

 doi:10.20944/preprints202410.1996.v1

incidents based on specific parameters (e.g. year, target area) is denoted as n, and the variance-mean ratio of the distribution with $D = \frac{\sigma^2}{\mu}$, where σ^2 is the variance and μ the mean.

4.1. Global Trends

Since 2001, the frequency of cybersecurity incidents targeting the GMTS has steadily increased, peaking in 2020 to coincide with the outbreak of the COVID-19 pandemic before declining slightly in 2021 then significantly increasing in 2022 and 2023. The adverse impact of the pandemic on the cybersecurity posture of organisations worldwide is well-known, with companies rapidly adopting remote working practices in response to legally-mandated lockdowns creating a particularly fertile environment for threat actors employing phishing and ransomware attacks against employees new to the remote workforce [17]. In a maritime-specific context, the increased difficulty faced by marine technicians in travelling to vessels and rigs due to COVID-19 travel restrictions led some organisations to intentionally lower their cybersecurity defences in order to allow remote service access to systems instead [18]. Figure 3 shows a chart of incidents per year globally in MCAD for which the year of the incident is known ($n = 291$). The significant increases in 2022 and 2023 are mostly attributed to ransomware as seen later on in Figure 9.

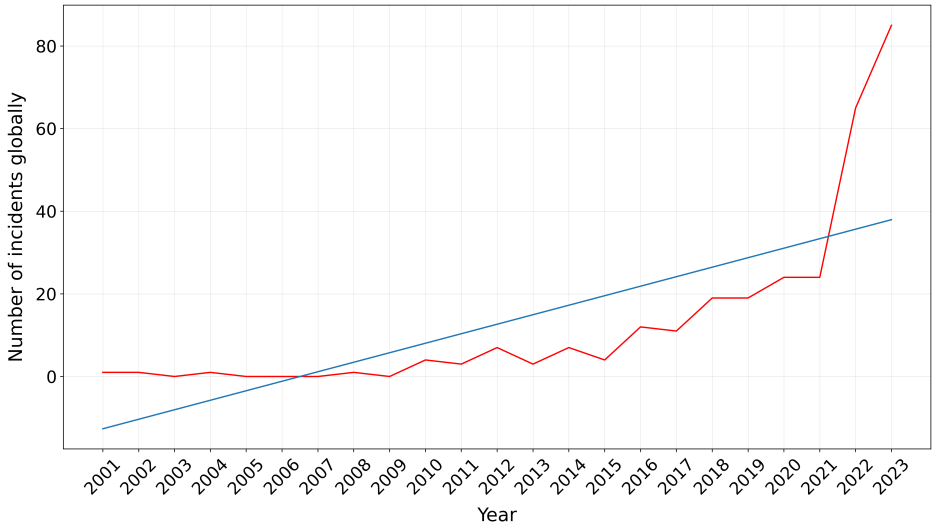

Figure 3. Frequency of maritime cybersecurity incidents globally per year from 2001-2023, showing a marked upward trend.

4.2. Asymmetry of Threat Actor and Victim Countries

Based on the analysis of the collected data, we note a marked asymmetry between the origin countries which threat actors emerge from when compared to victims. The variance-mean ratio of the distribution of incidents by *threat actor origin country* ($D = 9.71$) is significantly lower than when incidents are grouped by *victim country* instead ($D = 54.86$), indicating that a smaller group of countries originate a disproportionate number of threat actors targeting victims across a wider geographical area.

Figures 4 and 5 also illustrate this, with Russia, China, North Korea and Iran making up 80% of all incidents where threat actor origin country is known i.e. $n = 181$. By contrast, the top 4 victim origin countries (USA, UK, Germany and South Korea) make up just 40% of incidents where victim country is known i.e. $n = 306$ [2].

[2] This is larger than the number of incidents in our dataset, as some incidents note more than 1 victim origin country.

 doi:10.20944/preprints202410.1996.v1

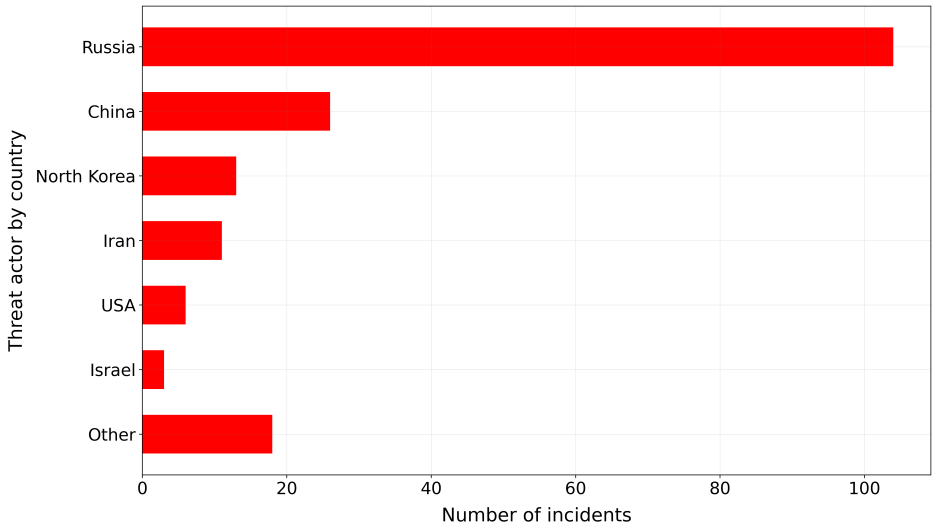

Figure 4. Frequencies of incidents originating with threat actors from different countries. Only incidents where threat actor country is known are included. Countries with threat actors originating fewer than 2 incidents are grouped as "Other".

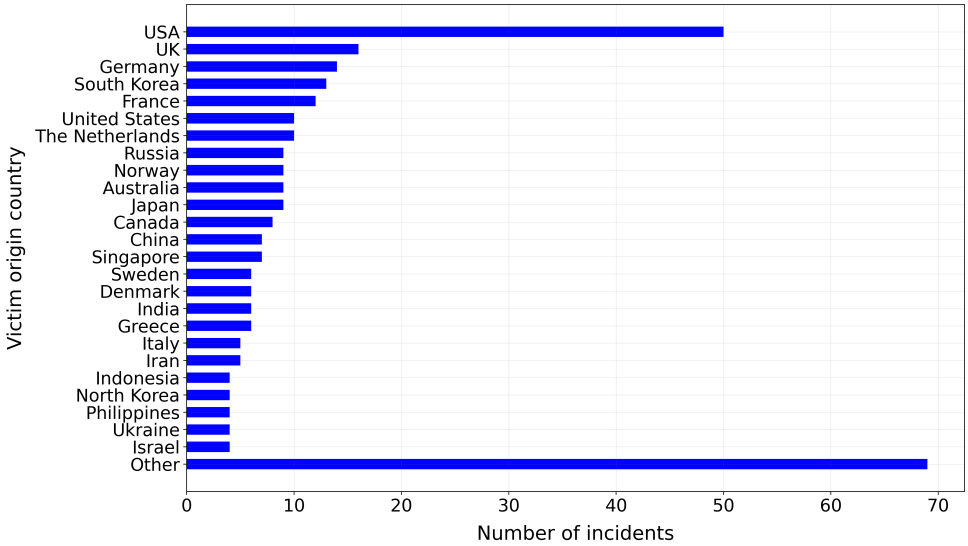

Figure 5. Frequencies of incidents targeting victim organisations from different countries. Only incidents where victim country is known are included.

While this finding is striking, it should be noted that data collection methodology is subject to limitations that may cause bias in our collected results. We discuss these limitations further in Section 5.1.

4.3. Year-on-Year Threat Actor Activity by Continent

Trends in the frequency of incidents over time by both threat actor and victim geography are also evident in the data. Prior to 2016, threat actors originating in Asia were responsible for the majority of incidents studied, while from 2016 onwards, Russian threat actors assumed an outsize role in the perpetration of cyber incidents worldwide. When compared to Asia and Russia, threat actors originating in Africa, Europe, Oceania and the Americas played a much smaller role, with the exception of in the year 2012, when a number of primarily domestic incidents (i.e. from US threat actors against US victims) appear in the literature. Figure 6 shows year-on-year frequency of cyber incidents grouped by threat actor origin geography between 2001 and 2023.

 doi:10.20944/preprints202410.1996.v1

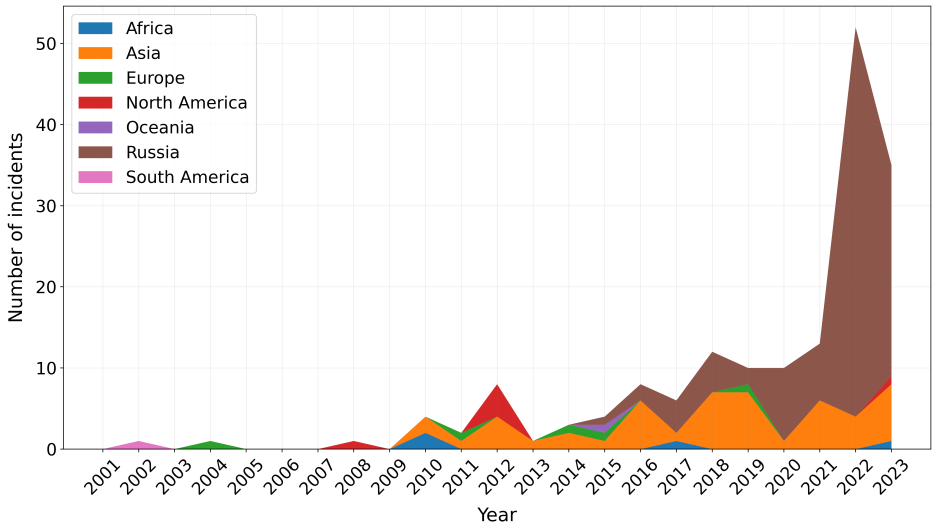

Figure 6. Proportion of incidents originating with threat actors by continent. Only incidents where threat actor country is known are included. As a transcontinental country with disproportionate representation in the data, Russia is plotted separately.

Victim geographies are much more uniformly represented in the data. Asia, Europe and North America are represented approximately equally, with African, Oceanian, Russian and South American victims targeted less frequently. Figure 7 illustrates the occurred cyber incidents between 2001 and 2023, grouped by the original location of victims, on a year-on-year basis.

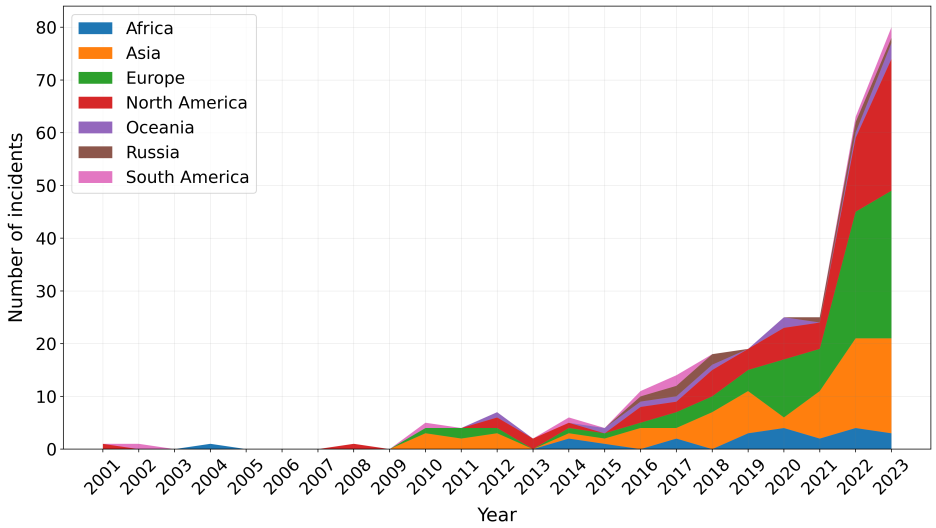

Figure 7. Proportion of incidents targeting victims by continent. Only incidents where victim country is known are included. As a transcontinental country with disproportionate representation in the data, Russia is plotted separately.

4.4. Attack Method

Ransomware comprises over a half (53%) of incidents in MCAD where the attack method is known ($n = 288$), and makes up the majority of incidents involving malware (87%), as seen in Figure 8. As with many other industries, maritime operations have become an attractive target for ransomware attacks due to lack of investment in cybersecurity and the potential for significant disruption in their operations [6,19]. Such attacks have a wide range of impact from vessel communication systems and navigation suites, to cargo management and logistic systems.

 doi:10.20944/preprints202410.1996.v1

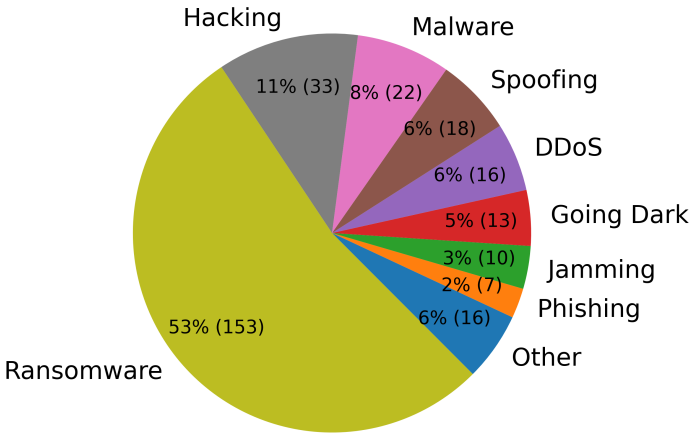

Figure 8. Proportions of incidents in MCAD employing different attack methods. Only incidents where attack method is known (and relevant) are included.

Another interesting observation are incidents categorized as "going dark". The term "going dark" refers to a practice whereby a ship intentionally disables their Automatic Identification System (AIS) transponders to evade detection and monitoring [20]. Crews may engage in this practice for several reasons including evading international sanctions, engaging in unauthorized fishing activities, or transporting illicit goods. Nation-states or vessel operators may direct vessels to go dark in order to bypass trade restrictions, which may otherwise attract a penalty under international law. Of the 13 instances of a vessel going dark recorded in MCAD, Chinese and Iranian vessels make up over half (53% and 30% respectively).

In Figure 9 we also see that the past six years, ransomware attacks have overshadowed all other methods of attacks, reaching an all-time high of $n = 68$ in 2023. In 2022 and 2023, a slight increase to DDoS attacks has also been reported, stemming mostly from threat actors in Russia (8) and Sudan (1) and Indonesia (1).

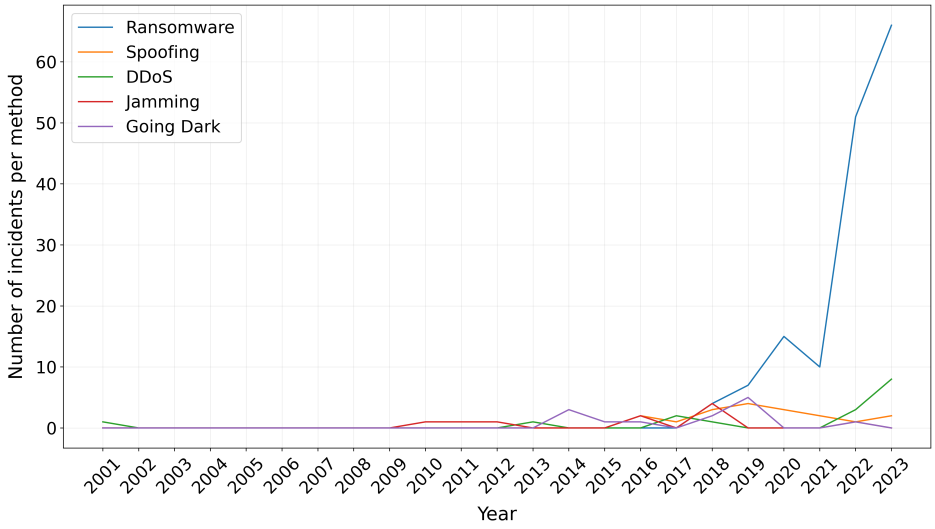

Figure 9. Frequency of incidents in MCAD involving five main attack methods.

5. Limitations & Future Work

While our work represents a first-of-its kind contribution towards facilitating information sharing around cybersecurity incidents affecting the GMTS, we acknowledge a number of limitations of our

 doi:10.20944/preprints202410.1996.v1

methodology and the MCAD software artefact itself that may impede the utility of MCAD or the completeness of the information in its database. Herewith we present our plans to address those limitations.

5.1. Limitations of Literature Review

Our own efforts to discover cybersecurity incidents affecting the GMTS in various forms of published literature (see Section 3), have proven effective in creating a rich and rigorously-researched starting point of over 290 incidents for the MCAD database. The continued effectiveness of this methodology, however, is limited by the number of researcher hours we are able to dedicate to the upkeep and curation of the data, biased towards cybersecurity incidents that are high-profile enough to enter the published record, and restricted largely to those that have information published in languages our researchers are familiar with (primarily English and Dutch). Language bias has been shown to be present in scholarly communication for several decades [21], and is of particular concern to projects such as MCAD, which aspire to present reliable information on a global scale.

Future work: We plan to make the data collection and curation process more scalable by employing some of the latest advancements in Natural Language Processing (NLP) technology such as Large Language Models (LLMs) [22] to create a AI-driven human-in-the-loop data pipeline from scholarly literature, news feeds and other sources of information on maritime cybersecurity incidents to MCAD. The powerful language translation capabilities of LLMs can also assist us in reducing language bias in the collected data.

5.2. Under-Reporting of Cybersecurity Incidents

It is well-established that efforts to compile statistics on cybersecurity incidents are significantly hampered by the tendency of cybercrime to go underreported, particularly by organisations motivated not to expose corporate weaknesses to their customers, shareholders or other stakeholders [23,24]. If cybersecurity incidents go unreported to law enforcement, they are less likely to either surface in the literature or be submitted to the MCAD via its self-report mechanism.

Future work: Our ongoing work to devise and deploy honeynets [25] provides a promising means to help address the issue of under-reporting of cyber incidents by victims. By deploying honeynets mimicking vessels, port authorities and other components of the GMTS, we can integrate incident data into the MCAD that does not ultimately rely on victim reports.

5.3. Lack of an Anonymous Reporting Mechanism

Individual employees that wish to report a cybersecurity incident suffered by their organisation may also feel unable to use the self-report feature of MCAD for fear or running afoul of corporate policy, violating non-disclosure agreements or otherwise facing repercussions for doing so. We have previously received enquiries about making anonymous reports to MCAD, which we had no choice but to decline, as we are currently unable to guarantee complete anonymity of either the individuals submitting reports to MCAD or the organisations those reports concern.

Future work: Although we do not have immediate plans to implement anonymous reporting functionality in MCAD, several potential approaches could be considered. One option is to use a separate secure server to receive anonymous reports, filtering out identifying metadata (such as sender IP addresses) before integrating the information into MCAD. Additionally, the self-report feature could be accessed through a Tor hidden service to ensure a better anonymity for users submitting incidents, providing an additional layer of protection for informants.

5.4. Lack of Visualisations for Key High-Level Statistics

MCAD does not currently feature any sort of dashboard showing key high-level statistics, or presenting these as visualisations of the type that we present in this work (e.g. Figures 3, 4 and 6). Other online cybersecurity incident dashboards tend to provide this functionality [26,27].

 doi:10.20944/preprints202410.1996.v1

Future work: We anticipate that this functionality will promote the adoption of MCAD as a CTI tool and facilitate further research utilizing it. To support this goal, we are in the process of adding dashboards to the application-similar to those presented in Section 4—which will be included in a near-future update.

6. Conclusion

In this work, we have presented MCAD, a user-friendly cross-platform CTI tool, backed by a curated database of over 290 maritime cybersecurity incidents. With the release of the MCAD, we aim to contribute to the cyber resilience of the GMTS by providing visibility to the significant global impact of maritime cybersecurity incidents, and providing researchers with a comprehensive tool. With MCAD as a reference point, researchers are able to facilitate practical studies, providing the necessary data to bolster the decision-making process of maritime organizations. We will continue to dedicate research effort towards the further improvement of MCAD, and future releases of additional application features and updates to the underlying database are planned. We believe that MCAD will continue to serve as a valuable resource for securing the maritime world.

Author Contributions: Conceptualization, J.P., S.M., S.J. and R.L.; methodology, J.P., S.M., S.J. and R.L.; software, S.J., R.L., and G.M.M.. and G.M.M.; validation, J.P., S.M. and G.M.M.; investigation, J.P., S.M.; resources, J.P., S.M., S.J. and R.L.; data curation, J.P., S.M. and G.M.M.; writing—original draft preparation, J.P., S.M., S.J. and R.L.; writing—review and editing, J.P., S.M., R.L., and G.M.M.; supervision, J.P., S.M. All authors have read and agreed to the published version of the manuscript.

Data Availability Statement: The original data presented in the study are openly available in the MCAD web application at https://maritimecybersecurity.nl.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ADMIRAL	Advanced Dataset of Maritime cyber Incidents ReleAsed for Literature
CTI	Cyber Threat Intelligence
CISSM	Centre for International and Security Studies at Maryland
EuRepoC	European Repository of Cyber Incidents
GMTS	Global Maritime Transportation Systems
GPS	Global Positioning System
JSON	JavaScript Object Notation
LLMs	Large Language Models
MCAD	Maritime Cyber Attack Database
NLP	Natural Language Processing
STIX	Structured Threat Information eXpression

References

1. Weaver, G.A.; Feddersen, B.; Marla, L.; Wei, D.; Rose, A.; Van Moer, M. Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach. *Transportation Research Part C: Emerging Technologies* **2022**, *137*, 103423. doi:https://doi.org/10.1016/j.trc.2021.103423.
2. Rifjay, D.N.N. European Union Efforts In Securing Cyber Environment Of Europe's Maritime Sector After Maersk Cyber-attack(2017-2018). PhD thesis, President University, 2021.
3. Ribeiro, A. Operations at Japan's Port of Nagoya resume, after probable LockBit ransomware attack. Industrialcyber, 2023. Available online: https://industrialcyber.co/transport/operations-at-japans-port-of-nagoya-resume-after-probable-lockbit-ransomware-attack/.
4. Oruc, A. Claims of state-sponsored cyberattack in the maritime industry. Conference Proceedings of INEC, 2020.
5. Schwarz, M.; Marx, M.; Federrath, H. A Structured Analysis of Information Security Incidents in the Maritime Sector, 2021, [arXiv:cs.CR/2112.06545].

6. Meland, P.H.; Bernsmed, K.; Wille, E.; Rødseth, Ø.J.; Nesheim, D.A. A Retrospective Analysis of Maritime Cyber Security Incidents. *TransNav, International Journal on Marine Navigation and Safety of Sea Transportation* **2021**, *15*, 519–530. doi:10.12716/1001.15.03.04.
7. Barnum, S. Standardizing cyber threat intelligence information with the structured threat information expression (stix). *Mitre Corporation* **2012**, *11*, 1–22.
8. Böhm, F.; Menges, F.; Pernul, G. Graph-based visual analytics for cyber threat intelligence. *Cybersecurity* **2018**, *1*, 16. doi:10.1186/s42400-018-0017-4.
9. Bronk, C.; deWitte, P., Maritime Cybersecurity: Meeting Threats to Globalization's Great Conveyor. In *Cyber Security: Critical Infrastructure Protection*; Lehto, M.; Neittaanmäki, P., Eds.; Springer International Publishing: Cham, 2022; pp. 241–254. doi:10.1007/978-3-030-91293-2_10.
10. Loomis, W.; Singh, V.V.; Kessler, G.C.; Bellekens, X. *Raising the colors: Signaling for cooperation on maritime cybersecurity*; Atlantic Council, 2021.
11. Tam, K.; Jones, K.D. Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy* **2018**, *3*, 147–164, [https://doi.org/10.1080/23738871.2018.1513053]. doi:10.1080/23738871.2018.1513053.
12. Bimco, International Chamber of Shipping, W.P.G., Cyber Security Workbook for On Board Ship Use; Marisec: London, 2023; p. 208.
13. Mraković, I.; Vojinović, R. Maritime cyber security analysis–How to reduce threats? *Transactions on maritime science* **2019**, *8*, 132–139.
14. Iqbal, Z.; Khan, M.K. Maritime cybersecurity: Vulnerabilities and counter measures. *Journal of Contemporary Studies* **2021**, *9*, 42–58.
15. Akpan, F.; Bendiab, G.; Shiaeles, S.; Karamperidis, S.; Michaloliakos, M. Cybersecurity challenges in the maritime sector. *Network* **2022**, *2*, 123–138.
16. Jacq, O. Détection, analyse contextuelle et visualisation de cyber-attaques en temps réel : élaboration de la Cyber Situational Awareness du monde maritime. PhD thesis, 2021. Thèse de doctorat dirigée par Kermarrec, Yvon Informatique Ecole nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire 2021.
17. Pranggono, B.; Arabo, A. COVID-19 pandemic cybersecurity issues. *Internet Technology Letters* **2021**, *4*, e247, [https://onlinelibrary.wiley.com/doi/pdf/10.1002/itl2.247]. doi:https://doi.org/10.1002/itl2.247.
18. Lohrmann, D. Is a 'Cyber Pandemic' Coming? https://www.govtech.com/blogs/lohrmann-on-cybersecurity/is-a-cyber-pandemic-coming.html, 2020. (Accessed on 05/13/2024).
19. Thetius, Cyberowl, H. Shifting Tides, Rising Ransoms and Critical Decisions: Progress on maritime cyber risk management maturity. Cyberowl, 2023. Available online: https://cyberowl.io/resources/global-industry-report-shifting-tides-rising-ransoms-and-critical-decisions-progress-on-maritime-cyber-risk-management-maturity/#download.
20. Bunwaree, P. The Illegality Of Fishing Vessels Going Dark And Methods Of Deterrence. *Cambridge University Press* **2023**, *71*, [https://doi.org/10.1017/S0020589322000525]. doi:10.1017/S0020589322000525.
21. Egger, M.; Zellweger-Zähner, T.; Schneider, M.; Junker, C.; Lengeler, C.; Antes, G. Language bias in randomised controlled trials published in English and German. *Lancet* **1997**, *350*, 326–329.
22. Vaswani, A.; Shazeer, N.; Parmar, N.; Uszkoreit, J.; Jones, L.; Gomez, A.N.; Kaiser, L.; Polosukhin, I. Attention is All you Need. Advances in Neural Information Processing Systems; Guyon, I.; Luxburg, U.V.; Bengio, S.; Wallach, H.; Fergus, R.; Vishwanathan, S.; Garnett, R., Eds. Curran Associates, Inc., 2017, Vol. 30.
23. Wall, D.S. Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime1. *International Review of Law, Computers & Technology* **2008**, *22*, 45–63, [https://doi.org/10.1080/13600860801924907]. doi:10.1080/13600860801924907.
24. Lydon, L. Corporate under reporting of cybercrime: Why does reporting to authorities matter? ISG MSc Information Security thesis series, Royal Holloway University of London, 2022. Available online: https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/.
25. Pijpker, J.; McCombie, S.J. A Ship Honeynet to Gather Cyber Threat Intelligence for the Maritime Sector. 2023 IEEE 48th Conference on Local Computer Networks (LCN), 2023, pp. 1–6. doi:10.1109/LCN58197.2023.10223347.
26. Harry, C.; Gallagher, N. Classifying Cyber Events: A Proposed Taxonomy. *Journal of Information Warfare* **2018**, *17*, 17–31.

 doi:10.20944/preprints202410.1996.v1

27. European Repository of Cyber Incidents (EuRepoC). Global Dataset of Cyber Incidents V.1.2, 2024. doi:10.5281/zenodo.11108195.