Identifying the Scope of Cybersecurity Research Conducted in the Maritime Industry: 2003 - 2023

Tshepo Mawer[1,2], Sune von Solms[1,2] and Johan Meyer[1]
[1]Department of Electrical and Electronic Engineering Science, University of Johannesburg, South Africa
[2]South African International Maritime Institute, Nelson Mandela University, Gqeberha, South Africa

tmawer@uj.ac.za
svonsolms@uj.ac.za
johanm@uj.ac.za

Abstract: The maritime industry plays a pivotal role in the modern economy, global trade, safety and transportation globally. Due to the rapid advancement and utilisation of technology in the field, the maritime industry is increasingly vulnerable to cybersecurity threats. The last decade saw many instances of infrastructure having been exploited or attacked, such as the maritime vessels themselves, the port infrastructure and the supply chain. Each component constituting the maritime industry requires unique system critical operations to ensure cybersecurity, however this paper focuses on certain aspects of the maritime industry only. As cybersecurity in the maritime industry is a growing field, this study determines the scope of cybersecurity research on maritime infrastructure which has been published to establish a baseline understanding of the current field. The paper presents the results from a systematic literature review conducted to assess the scope of current cybersecurity work published focusing on the maritime industry. The result from the study clearly shows the increased attention to cybersecurity in the maritime industry, which can be seen from the increased number of publications which showed a sharp increase after 2014.

Keywords: Cybersecurity, Maritime, Information security

1. Introduction

The history of seafaring and boat use dates to ancient times, serving various purposes like civilization mobility, exploration, trade, warfare, and fishing. Maritime sailing originated around the 3rd century BC, proving faster and more cost-effective for product transportation than land (Shipfinex, 2023). Container ships now move 90-95% of global manufactured goods, with the 2019 world shipping trade valued over $14 trillion (Di Fonzo & Paris, 2018). Navies and coast guards ensure safety in territorial waters, trade routes, and the environment, making the maritime industry a crucial global transport mode (Shipfinex, 2023).

Maritime activities significantly impact the world economy. The Suez Canal blockage in 2021 disrupted the global supply chain (Shipfinex, 2023). The maritime sector, undergoing modernization, faces growing cybersecurity threats with far-reaching consequences. It includes vessels, port infrastructure, and the supply chain, necessitating cybersecurity to ensure safety. Information and Communication Technology (ICT) is increasingly adopted for cost-effectiveness, safety, and sustainability, making cybersecurity a priority (Moan, 2022). Properly securing and managing ICT systems aboard ships, in ports, and throughout the supply chain is essential (Moan, 2022).

Cases of insecure systems or insecure operation have led to cybersecurity attacks, such as:

- A British tanker, Stella Impero, in the Strait of Hormuz took a sharp turn off course. It is then seized by Iranian forces in their waters. The ship's GPS location was spoofed. (July 2019).
- A cyber-attack against Transnet, who operates two major ports and most railways in South Africa, disrupted container operations at the ports of Cape Town and Durban. Operation capacity was reduced to 10% of normal operations, forcing workers to process cargo manually (July 2021) (Heiberg T., 2021).

With the increase of above-mentioned types of cyber incidents, the focus on cybersecurity in the maritime industry grows, and the question that emerges is whether the status of maritime cybersecurity in any manner reflects the production of scientific publications in this field? This study aims to analyse the scope of scientific publications in the field of cybersecurity in the maritime environment. This study provides an indication of the standing of cybersecurity research in the maritime environment that can serve as a baseline towards understanding the extent and scope of research conducted in the field. The paper is structured as follows: Section 1 includes the introduction where Section 2 provides a brief overview on the history of cybersecurity

and the maritime landscape. Section 3 provides a discussion on the methodology followed in this study with the results following in Section 4. Section 5 concludes this paper.

2. History of Cybersecurity and the Maritime Industry

The maritime industry continuously adapts to evolving technology, with ICT systems and advanced technology profoundly shaping a more interconnected and technology-dependent sector (Apud, 2016; Lind-Olsen, 2019). It involves advanced navigation systems using GPS, radar, sonar, computerized maps, control systems for electromechanical systems, radio and satellite-based communications, and Automatic Identification Systems (AIS). Modern ships, ports, and supply chains generate extensive data shared among various stakeholders (Apud, 2016; Lind-Olsen, 2019; Akpan, 2022; Alcaide, 2020).

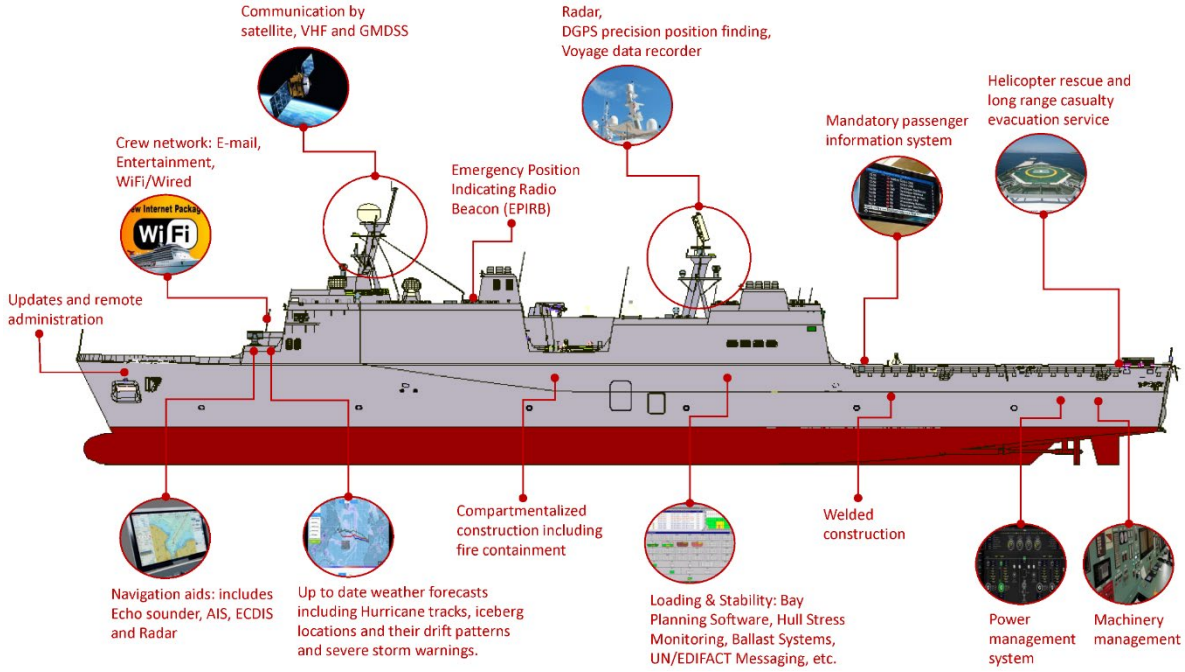

Figure 1: Automation systems for modern and autonomous ships (Akpan et al, 2022; CruisMapper, 2022)

The global rise in e-commerce and global shopping creates new opportunities for the maritime supply chain, not just for shipping and ports (UNCTAG, 2021). In 2020, the global commercial shipping fleet grew by 3%, totalling 99,800 ships with a gross tonnage of 100 or more. By January 2021, the combined capacity reached 2.13 billion dead weight tons. In 2020, ship deliveries fell by 12% due in part to lockdown-induced labour shortages, disrupting maritime-industrial operations. Most of the new ships were bulk carriers, followed by oil tankers and container vessels. To cope with limited vessel supply, owners and operators acquired second-hand ships with a mix of legacy and modern systems (UNCTAG, 2021).

Data generation and sharing as well as the utilisation of technology is not something new and plays a major role in many industries globally. However, the maritime industry and the related operations are unique because the maritime environment (Mouton, 2023):

- Spans a vast operational environment and limited connectivity.
- Includes the integration of operational technology (OT) and information technology (IT) systems.
- Includes a multitude of vessels and ports which uses legacy systems.
- Has a lack of standardisation and regulatory challenges.
- Suffers from supply chain vulnerabilities and insider threats.
- Suffers from limited awareness and training.

This unique environment raises cybersecurity issues for both modern and legacy systems. As more devices and systems are introduced into the broader network, the windows for cyber-attacks increase (Ignacio, 2021). This heightened connectivity renders the system more vulnerable to diverse cyber threats. In 2013, hackers took control of an oil rig's stabilizing system in the Gulf of Mexico, leading to a 19-day shutdown to rectify the dangerous tilt caused by the attack. In 2016, 280 Korean vessels experienced GPS jamming, resulting in navigation system shutdowns and receipt of false information (Chang, et al., 2019).

Cyber threats in the maritime industry are further compounded by the awareness of those involved in this space, emphasizing the need for additional research to address these vulnerabilities (Afenyo & Ceasar, 2023). While many companies within the maritime sector are working to enhance their cybersecurity measures, both the industry and academia recognize gaps in research, policy, standards, and personnel training (Afenyo & Ceasar, 2023). The maritime industry should develop cybersecurity protocols, enhance education and awareness, and promote further research to build on existing knowledge (Afenyo & Ceasar, 2023) (Chang, et al, 2019).

According to BIMCO guidelines (BIMCO et al., 2021; UNCTAG, 2021):

- Recognize cybersecurity threats, including internal and external risks.
- Identify asset weaknesses by listing onboard systems with communication links, ensuring all parties understand threats and protective measures.
- Evaluate risk exposure, vulnerability, and potential exploitation.
- Develop protective and detection strategies to reduce vulnerability impact.
- Create response plans with contingency measures for cyber risks.
- Efficiently respond and recover from incidents, assess response plan effectiveness, and update for changing threats (BIMCO et al., 2021).

As the focus on cybersecurity in the maritime industry is increasing, this paper tries to determine if the focus of cybersecurity in the maritime industry reflects in the production of scientific publications in this field? In order to determine the scientific publications published on cybersecurity in the maritime industry, a systematic literature review was conducted to determine the trends in research publications in the field.

3. Methodology and Information Sources

A systematic literature review (SLR) is a comprehensive and methodological approach to identify and collate publications and research that have already been conducted, tailored towards answering a specific research question or hypothesis (Xiao & Watson, 2019). The decisions and procedures for including or excluding certain publications are to be well defined and/or justified, to ensure that the review is repeatable (Mohamed Shaffril et al., 2020). Through the lens of a SLR one can discover the depth and breadth of the existing body of knowledge pertaining to a topic or research question, while identifying gaps that require further exploration (Xiao & Watson, 2019). By rephrasing the aim of this paper, the authors determined the research objective necessary for the systematic literature review – *To determine the scope of research published within the field of cybersecurity and the maritime industry.*

The PICO (Population, Intervention, Comparators, Outcome) methodology for conducting a systematic literature review (SLR) was used. This methodology entails defining the research question around the four parameters (from which PICO is derived) and utilising that framework to develop the search terms or combination of keywords that will be used in the database search (Purssell & McCrae, 2020). The methodology assists in narrowing the focus of the SLR to more of the relevant documentation, rather than focusing the research net too wide. A variation of this model was chosen, specifically the Population, Exposure and Outcome (PEO) method due to its focus on the exposure of the research rather than its intervention, as the aim of this paper was to establish what research had already been conducted (Purssell & McCrae, 2020). For this paper the PEO model looks as follows:

Population: This parameter represents the sample space that is being explored, which for this paper would be the *maritime industry.*

Exposure: This parameter represents the research within the maritime field that are cybersecurity related that have already been published, which for this paper would be the *cybersecurity.*

Outcome: This parameter represents the outcome which this study necessitates, which is to develop an understanding of the current *scope of research* that has taken place (as of this paper's publication) into *cybersecurity within the maritime context.*

In the SLR, the considered publications were restricted to journals, articles, and peer-reviewed conferences meeting specific criteria, including international reputation and English language. Two databases were chosen to ensure insightful results: IEEE Xplore, a digital library by the IEEE, covering engineering, electronics, and

computer science (IEEE Xplore, 2023); and Scopus, a multidisciplinary digital library with peer-reviewed literature, including journals, books, and conference proceedings (Elsevier, 2023). Scopus is the largest citation and abstract database with smart research analysis tools. IEEE Xplore and Scopus were selected due to their integrated tools for capturing and analysing published research (Elsevier, 2023).

The SLR process followed can be described by the following steps:

Step 1. The period of data considered for the SLR was not restricted.

Step 2. Research publications in English, peer-reviewed and of type journals, articles and conference papers were considered.

Step 3. Table 1, below gives the key words selected for the SLR.

Table 1: Table of search terms and their synonyms

Keyword	**Synonyms**				
cybersecurity	"cyber security"	"cyber-security"	"network security"	"information security"	"security of data"
maritime	marine				

For each database, two searches were conducted, shown below. The use of Boolean operators was vital in ensuring a controlled search across both databases, as well as the use of quotation marks in order to restrict the search to the relevant keywords/search terms.

String 1: (cybersecurity OR "cyber security" OR cyber-security OR "network security" OR "information security" OR "security of data") AND (maritime)

String 2: (cybersecurity OR "cyber security" OR cyber-security OR "network security" OR "information security" OR "security of data") AND (marine)

The first search included maritime as a keyword, which refers to anything related to shipping, navigation, or commerce of the sea (such as maritime law and maritime trade) (Youth Maritime Collaborative, 2023). Within the context of research, the term maritime is often linked to the design, innovations and technologies meant to enable better exploration, transportation and human endeavour upon the oceans and seas (Hildebrand & Schröder-Hinrichs, 2014). The second search replaced maritime with marine, which refers to anything related to the ocean or sea, such as marine biology or life (Hildebrand & Schröder-Hinrichs, 2014). Within the context of research the term marine often refers to the understanding and study of ecologies and ecosystems, human impact on those ecosystems and avenues to move forward with to enable sustainable use and growth NOAA, 2022).

Step 1. Publication search: The title, abstract and keywords of each publication in the search database were interrogated for the presence of the search terms. When the search terms were found, the following meta information from the publication was captured in the results database which included:

- Title of paper
- Year of publication
- Authors and affiliations
- Author and Index Keywords
- Name of conference proceedings or journal
- Abstract
- Digital Object Identifier (DOI)

Step 2. Exclusions: The following exclusion criteria were applied to the initial search results. Publications with primary focus on the terms indicated in Table 2, were excluded for the reasons stated:

Table 2: Exclusion terms

Exclusion term	**Reason for exclusion**
Ports and port infrastructure	Not in scope, focused on maritime vessels
Naval and naval vessels	Focused on commercial/civilian vessels, not military
Oil rigs/freight/container	Cybersecurity in the offshore exploration domain was not the focus of this study

Underwater communication networks/ submarine cables	Underwater communication systems utilised in the communication industry were not the focus of this study
Exclusion term	**Reason for exclusion**
Energy generation	Offshore energy generation platforms and systems were not considered
Inland rivers	Excluded research on inland shipping
Environmental monitoring systems **Internet of Underwater Things** **Underwater sensor systems**	Systems and sensors utilised for the collection of data regarding the marine environment were excluded
Marine farming	Publications with a focus on marine farming were excluded as the focus of this study was the maritime vessel
Laws, strategies and policies	Publications with primary focus on maritime policy or maritime law were excluded from this study

Step 3. Duplication Removal: Duplicate publications from the database search results were eliminated using two methods. Initially, the unique DOI was compared to remove duplicates. The second pass involved cross-referencing document titles and author names to further eliminate any remaining duplicates.

Note that this search does not include corporate or military research into cybersecurity in the maritime industry as this study considers the contribution of academic research from academic institutions. This search is not an exhaustive study as not all academic databases were considered in this study. However, the search was considered to be of sufficient size in order to provide trends in maritime cybersecurity publications.

4. Results

The data collection methods discussed in Section 3 were applied using the IEEE Xplore and Scopus databases. After an initial search the total amount of publications before scope and duplicate exclusions totalled 1336 publications. A total number of 487 publications spanning from the year 2003 till 2023 were obtained after out of scope and duplicate exclusions were removed. To obtain an overview of the scope of research conducted on cybersecurity in the maritime industry a number of data depictions were generated, each providing different insight into the domain of cybersecurity research in the maritime industry.

4.1 Number of Publications per Year

The number of publications per year in the maritime industry focussed on cybersecurity is an indicator of the interest given and research effort allocated to this field. The number of publications generated per year is shown in Figure 2.

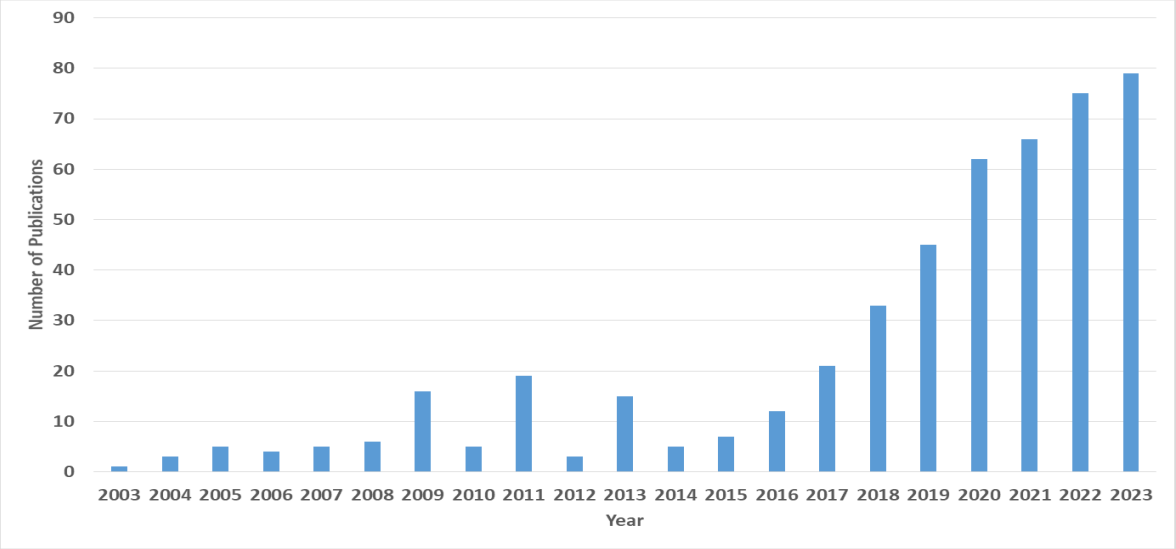

Figure 2: Number of publications per year over the entire study period from 2003 to 2023

The number of publications in the search field as function of year published is shown in Figure 2. The results showed that from the year 2003 until 2014 an average of about 7 conferences papers and/or articles were

published. From 2003 until 2008 the largest number of publications was a total of 6 publications in 2008. From the year 2008 until 2014 there were alternating years of similar amounts of publications and spikes in the amount of research published, with 2011 holding the largest number for that period of 19 publications. However, if one looks at the results from 2015 until 2023 an obvious trend is established, as there was a significant increase in the number of publications over that period of time. Starting with 7 publications in 2015 the number of publications increases to 79 publications so far for 2023. These results indicate a significant increasing trend in cybersecurity research in the domain of the maritime industry. An exponential increase of nearly 1029% is observed over the period from 2015 to 2023. The aim of this research was not to come up with a prediction of where these numbers might go in future therefore, a regression curve was not fitted to the data presented in Figure 2.

It is insightful to compare the growth in publications in cybersecurity in the maritime industry with the growth in the industry itself. The international maritime trade consisting of tanker, bulk and other dry cargo, has grown from 5 984 million tons loaded per year to a maximum of 11 071 million tons loaded in 2019 (United Nations, 2021). Although the maritime tons loaded more than doubled, the increase in cybersecurity around the maritime industry has increased more than tenfold showing how the interest in cybersecurity around the maritime industry has intensified as shown in Figure 2.

4.2 Number of Publications per Country

An analysis of the country affiliation of the authors from the publications provide insight into the countries conducting or collaborating in research related to cybersecurity in the maritime industry. Figure 3 shows the number of publications obtained from the SLR ranked by country affiliation of the authors.

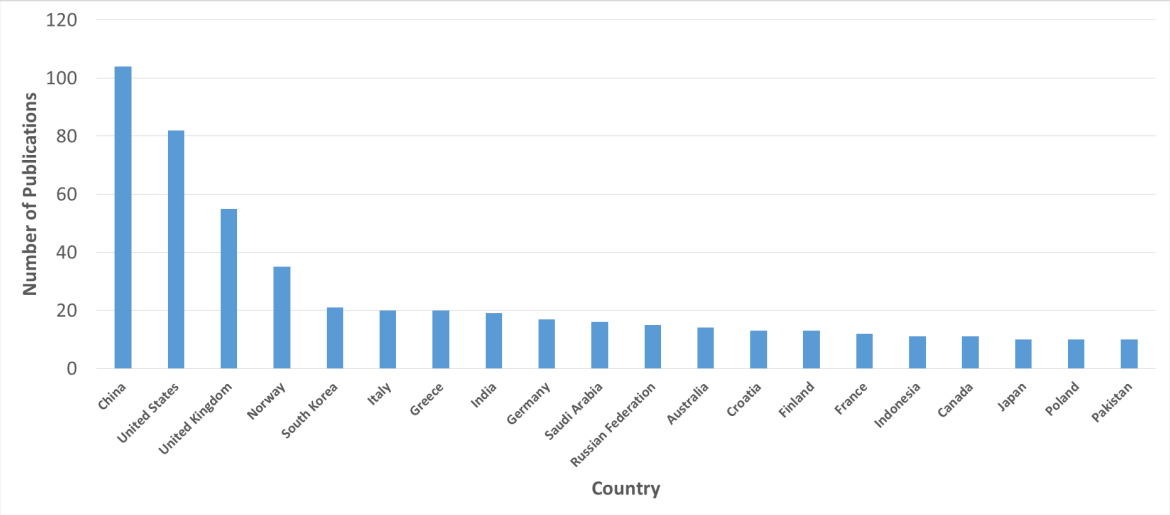

Figure 3: Number of publications per country over the entire study period.

The percentage share per region in world maritime trade (United Nations, 2021), may be indicative of the countries producing research in maritime cybersecurity. Asia with the highest percentage share (54% trade share) has also produced the highest number of publications namely 104 in total from China affiliated researchers with the Americas (18% trade share) second with 82 publications followed by European countries (15 % trade share) such as the United Kingdom and Norway producing 55 and 35 publications respectively. It is interesting to note that the combined number of research publications from China, United States and United Kingdom and Norway forms 41.69% of the total amount of publications produced globally.

Indicating the research publications numbers as generated per country on a global country heat map, provides a graphical indication of geo-located research in maritime cybersecurity. Figure 4 is a heat map of the number of research publications obtained by the SLR, geo-located on the global map.

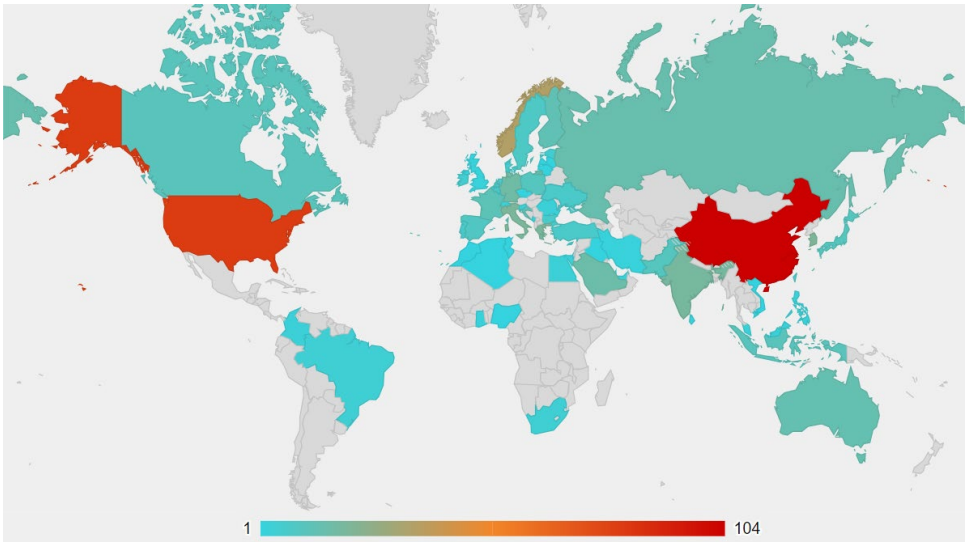

Figure 4: Number of research publications per country.

4.3 Cybersecurity Topics of Interest

Insight into the underlying topics of interest which was researched can be obtained by looking at the key words used to describe the research publications. Table 3 gives the frequency histogram ranked by occurrence, of the keywords used to describe the topics of interest.

Table 3: List of key word used to describe the research topics

Keyword	Frequency	Keyword	Frequency	Keyword	Frequency
Network security	203	Internet of Things	45	Marine transportation	27
Cybersecurity	152	Waterway transportation	41	Marine communication	23
Ships	128	Crime	36	Cryptography	22
Security of data	115	Risk management	34	Maritime industry	21
Risk assessment	81	Automatic Identification System	30	Maritime security	21
Security	64	Computer crime	28	Authentication	20
Cyber-attacks	50	Automation	27	Monitoring	20

Figure 5: Word cloud map of keywords over the full 21 years study period

It is no surprise that the top ranking three keywords are Network security (203), Cyber Security (152) and Ships (128). However, more insight into the underlying research field can be obtained by looking at the lesser ranked keywords. A word cloud with the word size as an indication of frequency of occurrence is shown in Figure 5. Using this means of representation is useful since it provides insight into the overall field of research in one glance. The lesser used topics of research are more easily represented in this form, and can be more easily compared to the more popular research topics.

4.4 Keywords per Year

An analysis of keyword usage per year gives an indication of the evolution of the research topics over the research period. Figure 6 shows how the emphasis on particular keywords used evolved over the study period. As the number of publications increased from the year 2015 so did the growth in the usage of the primary keywords.

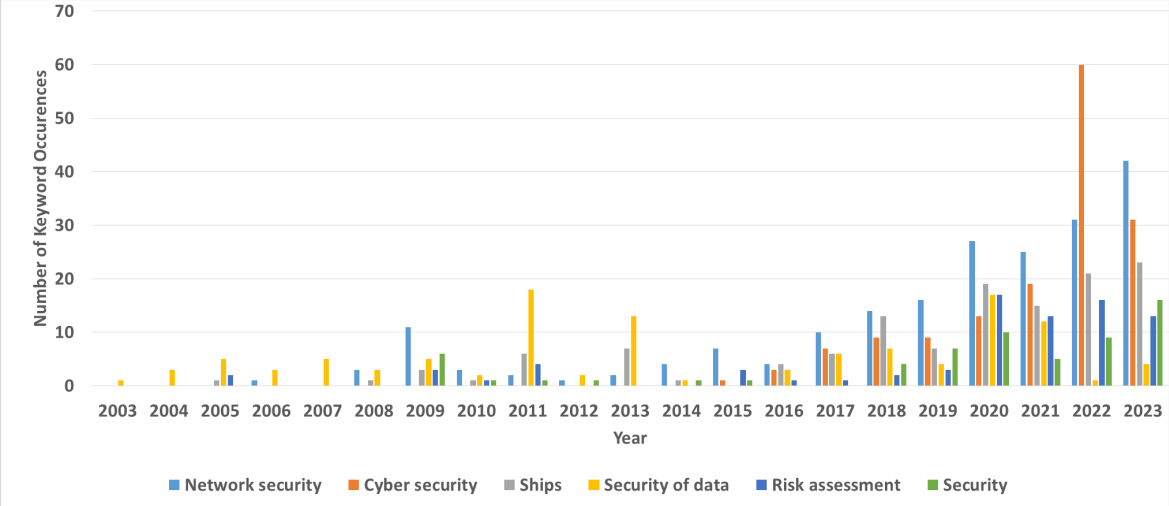

Figure 6: Number of keywords per year over the entire study period. For better visualisation the amount of keywords displayed is restricted to the top five keywords, as determined by the number of times those keywords appeared over the entire study period.

4.5 Top Keywords per Focus Area

An analysis of keyword usage per year gives an indication of the evolution of research topics over the research period. Figure 7 shows how the emphasis on particular keywords used evolved over the study period.

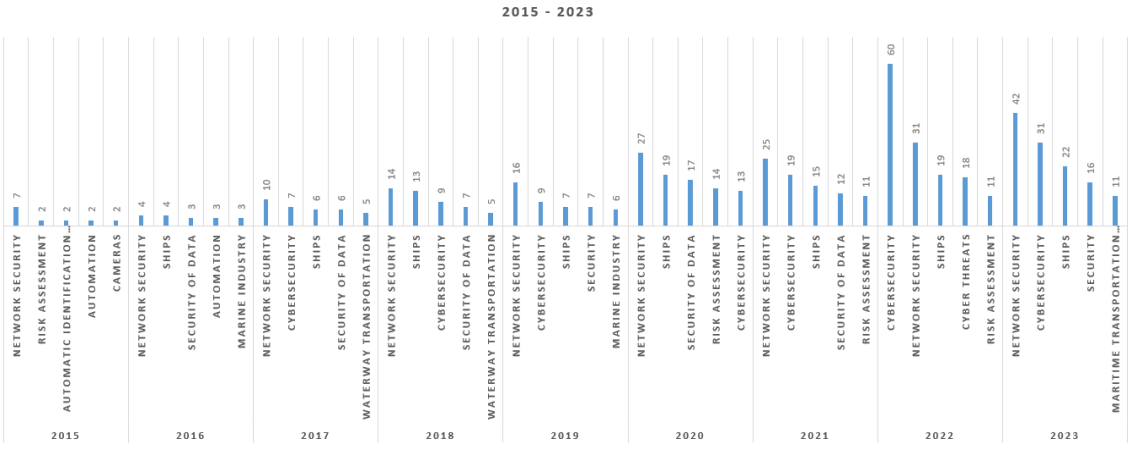

Figure 7: Growth in keyword usage over the period 2003 to 2023

From the year 2003 to 2015 there was a focus on the security of data and network security, through the appearance of keywords such as “Security of data”, “Computer networks”, “Risk assessment” and “Computer crime”. Other keywords such as “Global positioning system”, “Coastal zones”, “Marine engineering”, “Waterway transportation”, “Maritime security”, “Supply chains” and “Automation” can be found in the most frequently used search terms across those years as well. This indicates that cybersecurity and its maritime applications

were still in an earlier stage of development, as not only was there a smaller amount of research being conducted within these focuses, the content that did appear was primarily on specific systems within the maritime industry (such as those used in navigation or automation) as well as general risk assessment.

From 2016 to 2023 the top three keywords per year were always “Network security”, “Cyber security” and “Ships”, although the frequency with which they were used and the order in which they appear changed with time. This time period coincides with the surge of growth in research over the entire study period, and now it is clear that the focus area of many of those studies was specifically the protection of digital data and systems regarding ships. Other keywords that appeared frequently during this timeframe include “Automation”, “Waterway transportation”, and “Risk assessment”. This indicates that the need for research within cybersecurity and water transportation is still present, just the focus has shifted with time to be more general.

A similar trend can also be observed through the number of keywords used across each year of publications. Over the entire 20 year period for this study, the keywords used were tallied (which can be visually represented in Figure 5, as a word cloud map). “Network security” was the search term to appear the most, totalling 203 times. “Cybersecurity”, “Ships” and “Security of Data” showed up the most frequently after that, appearing 152, 128 and 115 times respectively. By separating these results by year it became clear that there was a significant increase in the number of these keywords from 2015 to 2023, as seen in Figure 7. These results follow a similar trend to that of the number of publications across that time period. Figure 7 also revealed that not every keyword was used over the whole 2003 - 2023 time period, with a large proportion of the keywords only being used frequently from about 2016.

5. Discussions and Conclusions

When reflecting on the history of cybersecurity in the maritime landscape it is clear that there has been an increase in the cyber-threats to the maritime industry over the last 21 years. The technology and systems being used in the maritime industry have been rapidly developing and evolving, however the cybersecurity systems in place have not developed as rapidly, or the integration of more modern systems with the existing legacy systems have led to greater opportunities for cybersecurity threats to exploit.

Through the lens of a systematic literature review this paper was able to gain insights into the scientific publications that have been developed over this period of rapid change. The number of publications per year over the period of study indicate a significant increase in research publications from about 2014, as well as an increase in the keywords associated with the maritime industry and cybersecurity in general. The most frequently appearing keywords being “Network security”, “Cyber security” and “Ships”, all of which saw a significant rise in used from 2015. The SLR also indicted that a vast majority of the research that had been published was from the United States, China, the United Kingdom and Norway. There was also a noticeable lack in published research from African countries as a whole.

In conclusion, when comparing the history of cybersecurity within the maritime industry to the insights and patterns found from the results of the systematic literature review it is apparent that there has been an increase in the attention paid to cybersecurity within the maritime industry, especially from 2014. This attention is reflected in the sharp increase in the number of scientific publications that have been produced in more recent years, as well as the significant increase in the use of keywords directly linked to cybersecurity and the maritime industry.

References

Alcaide, J.I.; Llave, R.G. (2020) “Critical infrastructures cybersecurity and the maritime sector”. Transp. Res. Procedia 2020, 45, 547–554.

Akpan, F., Bendiab G., Shiaeles, S., Karamperidis, S., Michaloliakos, M., (2022) “Cybersecurity Challenges in the Maritime Sector”, Network 2022, 2(1), 123-138

Apud, Julius Patrick, (2016) “Information Technology Applications in the Maritime Industry”, The Maritime Review, [online], https://maritimereview.ph/information-technology-applications-in-the-maritime-industry/

Chang, C-H, Wenming, S, Wei, Z, Changki, P and Kontovas, CA (2019) “Evaluating cybersecurity risks in the maritime industry: a literature review” International Association of Maritime Universities (IAMU), [online], https://researchonline.ljmu.ac.uk/id/eprint/11929

CruisMapper. Cruise Ship Safety. Available online: https://www.cruisemapper.com/wiki/751-cruise-ship-safety (accessed on 3 February 2022).

Di Fonzo, T. & Paris, LLC. (2018) “How a Steel Box Changed the World: A Brief History of Shipping”, WSJ Video, [online], https://www.wsj.com/video/series/a-brief-history-of/how-a-steel-box-changed-the-world-a-brief-history-of-shipping/CF460889-9984-483E-AF44-324330B89ECA

Elsevier (2023) “About | Elsevier Scopus Blog”, [online], https://blog.scopus.com/about#:~:text=Scopus%20is%20a%20source%2Dneutral,promote%20ideas%2C%20people%20and%20institutions

Heiberg T. (2021) “Transnet restores operations at ports after cyber attack”, CNBC Africa, [online], https://www.cnbcafrica.com/2021/transnet-restores-operations-at-ports-after-cyber-attack/

Hildebrand, L.P., Schröder-Hinrichs, JU. (2014) “Maritime and marine: synonyms, solitudes or schizophrenia?” WMU J Marit Affairs 13, 173–176 (2014). https://doi.org/10.1007/s13437-014-0072-y

IEEE Xplore (2023) “About IEEE Xplore”, [online], https://ieeexplore.ieee.org/Xplorehelp/overview-of-ieee-xplore/about-ieee-xplore

Ignacio de la Peña Zarzuelo, (2021) “Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue”, Transport Policy, ISSN 0967-070X, https://doi.org/10.1016/j.tranpol.2020.10.001

Lind-Olsen, Morten, (2019) “ICT solutions bring ship and shore closer”, Dualog, [online], https://www.dualog.com/blog/ict-solutions-bring-ship-and-shore-closer

Mawuli Afenyo, Livingstone D. Caesar, (2023) “Maritime cybersecurity threats: Gaps and directions for future research”, Ocean & Coastal Management, ISSN 0964-5691, https://doi.org/10.1016/j.ocecoaman.2023.106493

Moan, S. (2022) “The value of ICT in the maritime industry”, Dualog, [online], https://www.dualog.com/blog/the-value-of-ict-in-the-maritime-industry

Mohamed Shaffril, H. A., Samsuddin, S. F., & Abu Samah, A. (2020) “The ABC of systematic literature review: the basic methodological guidance for beginners”, Quality and Quantity, 0123456789. https://doi.org/10.1007/s11135-020-01059-6

Mouton, F. (2023) “Charting a secure voyage: Navigating social engineering in maritime”, NORMA Cyber Conference.

National Oceanic and Atmospheric Administration (NOAA), U.S Department of Commerce, (2022) “Marine Scientific Research”, NOAA, https://www.noaa.gov/marine-scientific-research

Paré, Guy, Marie-Claude Trudel, Mirou Jaana, and Spyros Kitsiou. (2015) “Synthesizing Information Systems Knowledge: A Typology of Literature Reviews.” Information & Management, 52:183–99. https://doi.org/10.1016/j.im.2014.08.008

Purssell, E. and McCrae, N. (2020) “How to Perform a Systematic Literature Review, How to Perform a Systematic Literature Review”, ISBN 978-3-030-49671-5. https://doi.org/10.1007/978-3-030-49672-2

Shipfinex, (2023) “Emphasis Of Maritime Industry On The World Economy”, LinkedIn [online] https://www.linkedin.com/pulse/emphasis-maritime-industry-world-economy-shipfinex/

UNCTAD (2021), “Review of Maritime transport”, https://unctad.org/system/files/official-document/rmt2021_en_0.pdf

United Nations. (2021) “Review of Maritime Transport 2021” ISBN: 978-92-1-113026-3 https://unctad.org/system/files/official-document/rmt2021_en_0.pdf

Xiao, Y., & Watson, M. (2019) “Guidance on Conducting a Systematic Literature Review. Journal of Planning Education and Research”, 39(1), 93-112. https://doi.org/10.1177/0739456X17723971

Youth Maritime Collaborative (2023) “What is Maritime?” [online], https://youthmaritimecollaborative.org/what-is-maritime