Bolbot, Victor; Kulkarni, Ketki; Brunou, Päivi; Banda, Osiris Valdez; Musharraf, Mashrura

Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis

Published in:
International Journal of Critical Infrastructure Protection

DOI:
10.1016/j.ijcip.2022.100571

Published: 01/12/2022

Document Version
Publisher's PDF, also known as Version of record

international journal of critical infrastructure protection 39 (2022) 100571

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

journal homepage: www.elsevier.com/locate/ijcip

Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis

Victor Bolbot [a,*], Ketki Kulkarni [a], Päivi Brunou [b], Osiris Valdez Banda [a], Mashrura Musharraf [a]

[a] Department of Mechanical Engineering, Marine Technology group, Research group on Safe and Efficient Marine and Ship Systems, Aalto University, Espoo, Finland
[b] Novia University of Applied Sciences, Turku, Finland

ARTICLE INFO

Keywords:
Maritime cybersecurity
Preferred reporting items for systematic reviews and metanalysis (prisma)
Maritime supply chain
Autonomous ships
Cybersecurity risk analysis

ABSTRACT

Ships and maritime infrastructure are becoming increasingly interconnected as the maritime industry is undergoing the industry 4.0 revolution. This development is associated with novel risk types such as the increased potential for successful cyberattacks. Several review studies have investigated the regulatory framework in connection to maritime cybersecurity, the vulnerabilities in maritime systems, potential cyberattack scenarios, and risk assessment techniques. None of them though, has implemented a systematic literature review and bibliometric analysis of the available academic research studies in the discipline of maritime cybersecurity. The aim of this review, therefore, is to offer a succinct description of the progress in academic research on the arising topic of maritime cybersecurity. To that end, we conducted a bibliometric analysis of maritime cybersecurity-related studies based on several metrics and analysis tools, identified the topics of academic research in this field, the employed methodologies and identified the main research challenges and directions in connection to maritime cybersecurity. To achieve the objectives, we employed principles from Preferred Reporting Items for Systematic reviews and Metanalysis (PRISMA) for systematic literature review and tailored keywords during a search in Scopus. The results demonstrated that Norway, the United Kingdom, France and the USA are the leading countries in maritime cybersecurity based on the weighted number of authors. The results also demonstrated that the main research focus in the area was on the development or application of cybersecurity risk assessment techniques and the design of monitoring and intrusion detection tools for cyberattacks in maritime systems. Based on the analysed literature, 53 challenges in various studies were identified and 73 topics for future research were suggested.

Abbreviation list

AHP	Analytical Hierarchical Process
AIS	Automatic Identification System
CAN	Control Area Network
DREAD	Damage, Reproducibility, Exploitability, Affected users, Discoverability
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
FMVEA	Failure Modes, Vulnerabilities and Effects Analysis
FTA	Fault Tree Analysis
GPS	Global Positioning System
HAZID	Hazard Identification
ICSRA	Integrated Cyber Security Risk Assessment
IMO	International Maritime Organisation
IoT	Internet of Things
ISO	International Standard Organisation
MaCRA	MAritime Cyber Risk Analysis model
MECE	Mutually Exclusive and Collective Exhaustive
MITIGATE	Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrAstrucTurEs
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PRISMA	Preferred Reporting Items for Systematic reviews and Metanalysis
RQ	Research Question
STPA	System-Theoretic Process Analysis
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
UK	United Kingdom
WMU	World Maritime University

* Corresponding author.
E-mail address: victor.bolbot@aalto.fi (V. Bolbot).

https://doi.org/10.1016/j.ijcip.2022.100571

Available online 30 October 2022

Introduction

As the maritime industry experiences the Industry 4.0 revolution, ships, systems onboard ships and the related infrastructure become more and more interconnected [1]. This is associated with several advantages such as remote and safe control of marine systems parameters, more accurate health status estimation for marine systems, improved human performance through closer cooperation amongst the ship and shore personnel, more accurate ship fuel consumption monitoring, faster identification of faults and faster and more precise decision-making, facilitated cargo monitoring, more transparent compliance to exhaust gases emissions' regulations and more decentralised operations [2]. Furthermore, the increased connectivity constitutes a key enabler for more automated and crewless processes [3], pushing ship operations into completely new realms.

However, these benefits are accompanied by several challenges, with the most eminent related to increased cybersecurity risks [4, 5]. Ships constitute assets of significant value or strategical importance in a number of civil and military operations [6, 7]. Therefore, it is not a surprise that a number of cyber incidents have been already reported in the maritime industry with many more cyber incidents remaining unreported due to concerns with negative publicity [5, 8, 9]. One of the most prominent examples is the cyberattack on Maersk, resulting in enormous financial losses for the company even if it was an untargeted attack [10]. The breadth and intensity of cyberattacks are expected to increase in the future considering the developments in shipping and overall industry evolution in post-COVID-19 era [2, 11].

Unsurprisingly, maritime cybersecurity has been an area of intense research with several literature reviews published. Oruc, et al. [12] provided an overview of international standards, International Maritime Organisation (IMO) regulations and testbeds relevant to the ship navigation system cybersecurity assessment. Ben Farah, et al. [13] systematically reviewed cyberattacks in the maritime systems and identified several solutions that can be used to mitigate the impact of cyberattacks. Tusher, et al. [14] investigated the existing cyber risk assessment studies for autonomous ships. Ashraf, et al. [15] surveyed the cyber threats in the realm of maritime Internet of Things (IoT). Kessler [16] provided an overview of technical vulnerabilities in the Control Area Network (CAN) used on ships. Larsen and Lund [17] conducted a systematic review of studies on the cybersecurity perception in maritime. de la Peña Zarzuelo [18] provided an overview of challenges related to cybersecurity management in ports. Progoulakis, et al. [19] reviewed available standards and maritime sector guidance, insurance frameworks, risk assessment methods and risk controls measures. Adams, et al. [20], Adams, et al. [21] briefly reviewed the cybersecurity approaches to cyber risk management in ports. Bocayuva [22] investigated the general aspects related to port cybersecurity. Caprolu, et al. [23] provided a list of vulnerabilities and cybersecurity barriers for ship systems. Kavallieratos, et al. [24] investigated various alternative cybersecure architectures for cyber-enabled ships. Ahvenjärvi, et al. [25] reviewed the challenges associated with communication of cybersecurity aspects based on the system safety control structure for a remotely controlled vessel. Shapiro, et al. [26] examined the risks of Trojan horse attacks in the maritime transportation system. Silverajan, et al. [27] provided a list of vulnerabilities and control measures for unmanned ships. Botunac and Gržan [28] presented the software threats to the Automatic Identification System (AIS). You, et al. [29] investigated the cyber security risk assessment techniques and their applicability to the maritime transportation system.

These review studies aimed at understanding the general cybersecurity challenges in the maritime, identifying known system components' vulnerabilities, investigating maritime regulations and class society rules that are available for effective cybersecurity management, standards that can be used for ship cybersecurity assurance, locating cyber risk assessment techniques that can be applied to the maritime systems and, the protection mechanisms (control barriers) that can be used against cybersecurity attacks. Essentially, these studies focused on the practicalities related to cybersecurity risk assessment and management in the maritime ecosystem and therefore were less research orientated. None of the currently available review studies implemented a comprehensive analysis and a thorough bibliometric analysis of the research studies published on the topic of maritime cybersecurity. There is a need for a review which would offer a succinct description of the progress in the arising topic of maritime cybersecurity, would summarise the current state of knowledge with focus on the scientific methods and would distil the findings provided in the various research papers with focus on the future research and known methodological challenges.

The aim of this review is therefore to attempt to answer the following Research Questions (RQs) related to maritime cybersecurity research, which were not answered before:

- RQ1: What are the leading countries, authors, time progress, journals, and cluster topics in connection to maritime cybersecurity based on scientific publications' bibliometric analysis?
- RQ2: What common themes or categories can be found across the research studies for maritime cybersecurity and what scientific methodologies are used across these studies?
- RQ3: What methodological challenges are reported in these studies and what future research directions do they lead to?

The RQ1 aims at identifying the achieved progress in the topic of academic maritime cybersecurity in different countries, journals and established networks of cooperation, RQ2 at the employed scientific methods and common themes and RQ3 at the known challenges and potential future research in the area. In this way, a succinct description of the progress in maritime cybersecurity and future research directions can be realised which is of great support for novel and experienced researchers in the field.

The novelty of the present study stems from the multitude of conference papers and journal articles that we analysed and the breadth of the conducted review in comparison to the previous reviews. Unlike the previous studies, we follow a systematic literature review methodology, we implement a bibliometric analysis and investigate RQs which have not been answered in the previous studies. The scope of the conducted analysis is limited to the Scopus indexed peer-reviewed academic publications. The results depicted in the paper can be used to determine the effectiveness of public policy with respect to investment in academic research and to support establishment of cooperation between different identified research groups. The identified and analysed research studies, methodological challenges and the proposed research directions can support conducting innovative research.

This article is structured as follows. First, the literature review and bibliometric analysis methodology are presented. Then the investigated research questions are answered using the presented methodology. The paper's limitations are also provided. Lastly, we summarise the main review findings in the conclusions section.

Methodology

The review methodology of this article was based on Preferred Reporting Items for Systematic reviews and Metanalysis (PRISMA) [30], which is a structured method for conducting a systematic literature review. There are numerous other literature review techniques [31], but we preferred PRISMA as it is a widely used, systematic and easy-to-follow approach [32]. Here, we adapted the PRISMA methodology to answer the research questions presented in the introduction section. The information flow based on the PRISMA methodology is provided in Fig. 1 and the steps are elaborated in the subsequent sections. In the same figure, we also present the number of identified and finally selected publications.

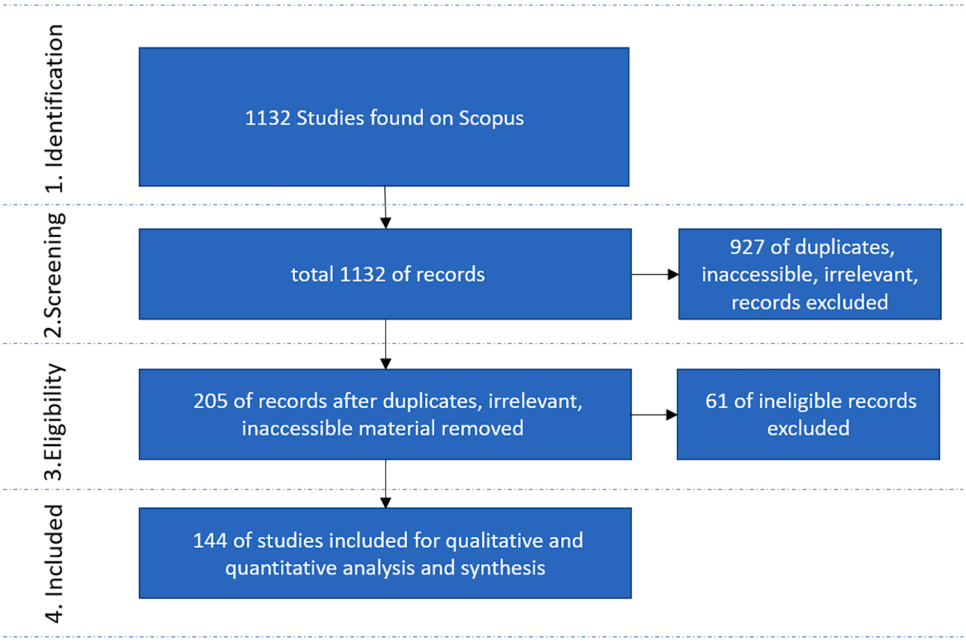

Fig. 1. The flow of information through the different phases of systematic literature review (Reported numbers valid as of 20th of July 2022).

Step 1: Identification of research studies

The identification of the relevant studies was implemented using Scopus as the search engine. We decided to exclude Google Scholar as the generated results using that search engine included multiple low-quality publications, which were not peer-reviewed or aimed at a more general audience (not academic as we targeted) and contributed to the diffusion of the conducted research. Also, we decided not to conduct the identification for the relevant publications in a series of journal publishers as the returned results were overwhelmingly large in number including many irrelevant publications. For instance, from Taylor and Francis for the term "maritime cyber security" we received 1637 entries in response, more than we totally checked using Scopus, and most of them were found to be irrelevant. Also, most of the journals at Elsevier, Taylor and Francis, Wiley and MDPI were indexed in Scopus. Therefore, the journal articles identified using Scopus would also be found on the relevant publishers' websites when similar search terms are used. It is difficult to specify whether Scopus is more or less suitable than the Web of Science for the identification purposes [33]. Still, there is some indication that Scopus offers a broader coverage for major fields than Web of Science [33]. Therefore, by using Scopus we ensured broader coverage compared to what we would cover using Web of Science.

For the identification generic keywords as below were used:

- maritime cybersecurity,
- maritime cyber security,
- ship cybersecurity,
- ship cyber security
- port cybersecurity
- port cyber security

We decided to use the word cyber security and cybersecurity in combination with other words during identification as the observant results, although largely similar, included some additional valuable references. Also, it was noticed that the first two keywords (maritime cybersecurity and maritime cyber security) contributed to the identification of the most research studies that were included in this analysis (126 out of 144 or 88%), even though it resulted in a rather limited number of totally found studies on Scopus (388 out of 1132 or 34%). So, when additional keywords (ship cybersecurity/cyber security, port cybersecurity/cyber security) were used, significant number of additional studies was identified. However, very few research studies were additionally included for these keywords (ship cybersecurity/cyber security, port cybersecurity/cyber security), only 18, much less than using the two first keywords, as most of them had been already included using the first two keywords. Considering this convergent behaviour, we did not perform research in Scopus for additional keywords which could be additionally considered (vessel cybersecurity, autonomous ships cybersecurity, etc.).

Step 2: Screening of research studies

Screening was implemented to reduce the number of identified publications to allow a more thorough analysis of the most relevant ones. Screening was achieved by reading through the publications' title, publication's abstract and, if necessary, a quick reading through publications' contents. This was done by considering whether the research study investigated maritime ecosystem cybersecurity as a whole or through its elements, how much text was allocated to the maritime ecosystem cybersecurity problems or system, and how much the maritime cybersecurity was enhanced. Also, duplicate references were identified and eliminated during this analysis step. We also excluded books from this analysis, as they offer retrospective opinions on the subject, are not so easily accessible and to the large extent cite findings from previously published conference papers and journal articles. Based on the screening, many of the initially identified research studies were excluded (retention rate of 205/1132 or 18%). A limited number of relevant studies were unfortunately inaccessible and had to be excluded.

Step 3: Eligibility assessment of research studies

During the eligibility analysis, the screened studies were further analysed and the most suitable were selected for further processing. This was implemented using the following criteria: the publication source (whether it was published in a credible journal or not), the significance of contents (such as practical implications and whether significant effort to derive some innovative results was realised), the soundness of the research methodology and results (whether some meaningful and rational methodology was applied and whether conclusions were meaningful). For assessing the publications coming from journals we

took into account the journal rankings suggested by Scimago [34] and excluded journals belonging to Q4, so very few Scopus-indexed journal publications were excluded. This was implemented to ensure that the good quality research studies receive their proper attention. We did not exclude the conference papers as a group from the analysis, as during the review we found important and interesting contributions presented at conferences. For assessing the conference papers, we applied the criteria referred above. In this step, we were rather tolerant and practically most of the research studies that were screened were included for the analysis (144/205 or 70%). This was implemented to incorporate as broad perspectives as possible in the analysis and to have adequate material to answer the research questions and conduct bibliometric analysis. An overview of the selected research studies is provided in tabular format as part of Appendix A, where their basic characteristics are specified.

Step 4: Included research studies analysis

During the last step, the eligible and selected studies were analysed in further detail. Only these research studies were used for answering the research questions. The analysis process is presented in the subsequent sections.

RQ1: What are the leading countries, authors, time progress, journals and cluster topics researching maritime cybersecurity based on scientific publications' bibliometric analysis?

To identify the impact of each country we considered the following scores/metrics for the included research studies.

1 The total number of authors that were included in all the papers and from each country, weighted by the number of publications in all 144 publications.
2 The number of each country's first authors, weighted by the number of publications.

Therefore, for the analysis, if an author from one country contributed to several papers x, then his/her contribution was counted x times. So, we did not estimate the number of unique authors but rather weighted the number of unique authors by the number of papers they have published, when considering contribution for each country. Also, we considered each author's affiliation at the date of publishing as referred to in the paper and not the actual nationality as the basis for the analysis. In case double affiliation was referred for the author, then each referred country took equal merit, i.e., its metric was increased by 1 for the first metric. However, for the first authors in the second metric, only the first affiliation was counted. Microsoft Excel was used for this analysis.

We also investigated the most prevalent journals that included publications on the topics related to maritime cybersecurity. For that, we used the number of published articles as a metric, without considering the number of citations they received, as they do constantly change and are also dependent on the publication year. Since we used Scopus as our main database and applied eligibility assessment based on Scimago ranking, only Scopus indexed references and top journals were included in the analysis.

We also implemented a historical analysis of publications to identify the attention researchers pay to different topics in the maritime cybersecurity. For that, we used the results of the analysis presented in the next RQ (RQ2) for the studies classification and used the number of publications per year on each research topic to identify historical trends.

Since the collection of articles included 144 documents, a bibliometric analysis was deemed feasible as well. Using the open-source software VOSviewer [35], co-authorship, and term analyses was conducted. The co-authorship analysis was used to determine the cooperation networks and term analysis to identify topics that are investigated by the researchers.

For the co-authorship analysis, there are two options available in VOSviewer: full and fractional counting. In the full counting method, every author of a co-authored article gets assigned the same score (weight) while counting the weights of links. In the fractional counting method, weight is counted as a fraction of the number of authors in an article. For example, if an article has 10 co-authors, each author is assigned 1/10 as the weight. To analyse the network in further detail, it is possible to view the biggest connections (a piece of the whole network that is fully interconnected and has the highest weights) separately. Both full counting and fractional counting can yield different results offering different perspectives with divergence increasing with the dataset size. In the full counting method, a small number of publications by a large group can have a dominant effect on the network [36]. This effect is reduced in fractional counting. Thus, the fractional counting method was preferred in this article.

For a term analysis, the full counting method counts the number of occurrences of a term in the articles. In the binary counting method, a score is assigned on whether a term is present or absent in the article, regardless of the number of occurrences. By default, 60% of the keywords were chosen to be displayed in the figures. This can be manually increased to include the full set. It is again possible to view the entire network with all keywords or to display the biggest network pieces. The full counting method was chosen here, to give more weight to the keywords that are mentioned more often.

RQ2: What common themes or categories can be found across the research studies for maritime cybersecurity and what scientific methodologies are used across these studies?

This constituted a more intricate part of our analysis, as there is no straightforward approach for research studies classification. The approach here resembled a puzzle-solving process. Once the investigated studies were aggregated, the first classification attempt was implemented using some criteria such as the publications' aim, the employed methodology, the investigated and considered systems and addressed problems. Then a second attempt was implemented, where the Mutually Exclusive and Collectively Exhaustive (MECE) principle was applied to the extent possible for the studies' grouping. To that mean, the term analysis presented in the previous section was of great help as it was used to verify the different study categories of classification, even if this information was rather of auxiliary nature. In cases where the paper was falling into two or more categories, we re-evaluated the major contributions and novelty of the paper before assigning it to a group based on the amount of text and the effort in a topic. The classification into various categories was supported by the use of definitions provided in standards such as NIST and ISO and the critical questions pointed by the reviewers of this paper during the review process.

The derived classification was used for the reporting of the found studies, for the identification of research study characteristics, for lower-level classification of methods and for identification of associated challenges and research directions in RQ3.

RQ3: what methodological challenges are reported in these studies and what future research directions do they lead to?

This constitutes the last, but not the least contribution of this article. For the identification of challenges introduction, methodology rationale and limitations/discussion sections of the investigated publications were carefully read, but relevant information from other sections was also included. To identify the directions for further research we rehearsed one more time the considered studies with emphasis on the discussion, conclusions, and future research sections. We employed the classification found from the previous research question (RQ2) to present the results. The identified challenges, research topics and directions were presented in a numbered list for better traceability and communication of the potential research directions.

Results and discussions

RQ1: Bibliometric analysis of the considered studies with respect to leading authors, co-authorship analysis, leading countries, journals, cluster topics and historical trends

The leading research countries based on the considered metrics (total weighted number of authors and the weighted number of first authors in the selected papers) are provided in Fig. 2 and Fig. 3 respectively. Due to the multitude of identified countries (44 in total), only the legends for the top 14 countries are provided in Figs. 2 and 3. As it can be observed, countries such as Norway, the United Kingdom (UK), the USA and France contributed the most according to both metrics (total weighted number of authors and the weighted number of first authors in the selected papers) in the considered period. The first 8 out of 40 (20%) finally identified countries (Norway, UK, USA, France, Croatia, Greece, Germany, South Korea) contributed the most to the research in maritime cybersecurity based on the metrics (66% and 69% retrospectively) and considering the selected Scopus-indexed publications. This is close to the well-known Pareto rule which states that 80% of the final output is produced by 20% of the total input [37]. Also, the two metrics gave similar results supporting the validity of this finding.

The most prevalent journals based on the number of selected Scopus-index publications on maritime cybersecurity are provided in Fig. 4. As observed, TransNav (the International Journal on Marine Navigation and Safety of Sea Transportation) accommodated most of the journal articles considered in this review. This journal is followed by the Journal of Marine Science and Engineering from MDPI in Fig. 4. Many of the Scopus-indexed studies were published in the Lecture Notes of Computer Science, which have also been included in Fig. 4. Fig. 4 Several other journals reported publications on maritime cybersecurity such as Sensors, Journal of Transportation Security, and World Maritime University (WMU) Journal of Maritime Affairs. Many scientific publications on maritime cybersecurity were also published in the IEEE transactions as can be observed from Fig. 4.

Fig. 4 indicates that the authors prefer to publish in a large variety of journals. This could be an indication of the lack of highly focussed journals on maritime cybersecurity. Considering the novelty of the issue, (as elaborated in Fig. 5), this should not be of surprise.

The analysis of historical trends is presented in Fig. 5. As observed, the number of publications only began to increase in 2017, indicating that the research topic only recently received appropriate attention. The steady increase in the number of articles since then indicates the growing significance of this field. It is observed that diversity of topics and methodologies (elaborated further in the next section) investigated in the maritime community is also increasing with time.

Figs. 6 and 7 present results from the bibliometric analysis using VOSviewer. Fig. 6 shows the co-authorship network. Of all the authors of the 144 articles, authors with at least 2 articles affiliated with their names were chosen. This resulted in the inclusion of 68 out of the 401 unique authors satisfying this criteria (17%), indicating that the vast majority of the researchers generated a rather limited number of Scopus-indexed publications on maritime cybersecurity. As mentioned earlier, the fractional counting method was preferred, since it reduced the impact of a small number of papers from a large group over the entire network. The results show one big cluster of authors along with multiple smaller clusters. Papastergiou, Mouratidis, Polemi, and others form the core of the biggest cluster, in the centre of the network. These researchers were affiliated with Greece; however, they were also interconnected with the researchers from Norway and UK. The other clusters are isolated from the centre as it seems that the researchers, or at least their publications were isolated from each other and each research group from different countries conducted mostly independent research. This can be attributed to the novelty of the research topic. This hopefully will change in the future as more research is implemented and more collaborative projects are pursued.

Also, it might be noted that most of the researchers referred to in Fig. 6 (who are constantly publishing in Scopus-indexed reference sources) are located in Europe. Very few researchers are coming from the other regions (Asia, America, Africa). Considering the results from Fig. 2 and Fig. 3 we can conclude that despite the significant research in the USA and other non-European countries, the academics that persistently rehearse the topic and publish have been in the European continent so far. As discussed in the problems with validity section, the present conclusion does not depict the intensiveness and steadiness of industrial research though.

Fig. 7 demonstrates the results of the co-occurrence of terms analysis. The full counting method was used, instead of the binary counting method, to give more weight to the keywords occurring more frequently. A total of 771 keywords were identified, of which generic terms were filtered out and only 89 terms were retained. The term analysis shows links between terms (keywords) commonly occurring

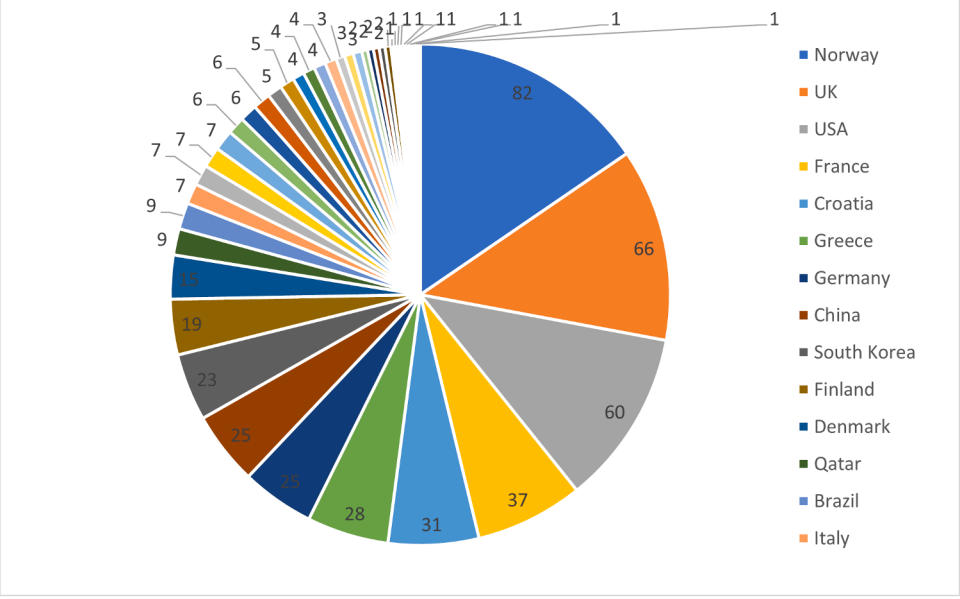

Fig. 2. The total weighted number of authors for top countries.

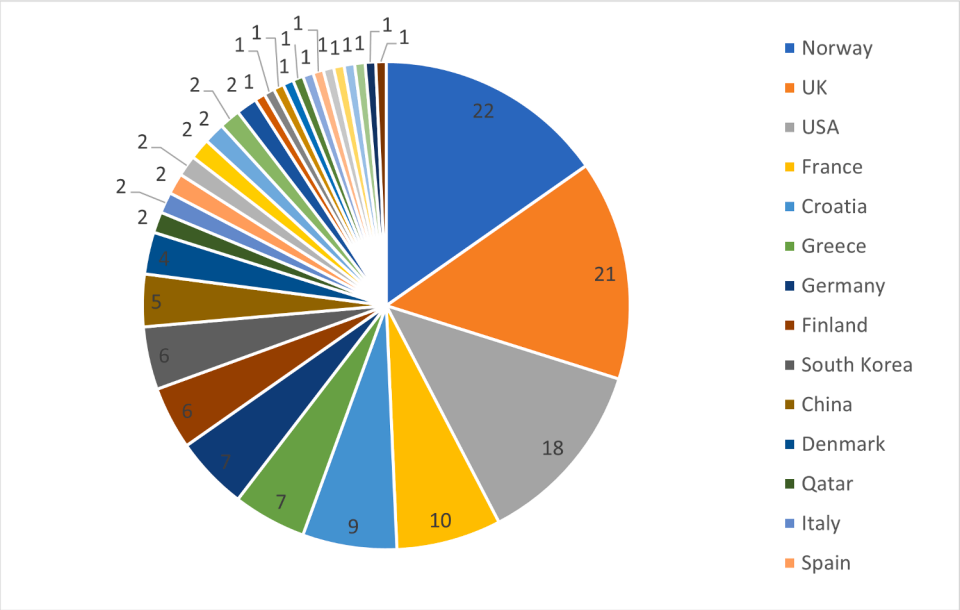

Fig. 3. The weighted number of first authors for top countries.

together. Apart from the obvious terms such as cyber risk, maritime sector, digitalisation, security and management, other frequently occurring terms include autonomous vessels (automation and other variants as well), ports, vulnerability and intrusion detection, maritime supply chain and various maritime systems. A closer look at the keyword analysis also indicates that researchers frequently discussed methodology, case studies and frameworks. Researchers seemed to be concerned with the issues associated with uncertainty, risk evaluation, situation awareness, the applicability of different methods, the relationship between safety and security, various attack types and COVID-19-generated issues.

RQ2: Categories of research studies

An overview of identified research study categories

For the categorisation of the research studies, we used the different definitions provided for the risk assessment in ISO 31,000 [38] and NIST [39, 40], vulnerability assessment in CISSP handbook [41] and NIST glossary [42], threat modelling in NIST SP800–53 [43], penetration testing in NIST glossary [44, 45], cyber incidents analysis in [46], resilience[47] and previous review studies on the topic such as [48]. Based on the term analysis results and definitions provided, we categorized the research studies as follows (also in Fig. 8):

1 Cyber risk assessment and treatment studies – Studies implementing risk identification, analysis, evaluation and treatment of cyberattack scenarios on ships, ship systems and maritime ecosystem. Into this category we also included studies, which focus on threat modelling, as threat modelling is part of risk assessment [43]. We also included studies focusing on vulnerability assessment, as vulnerability assessment is very frequently used as a part of risk assessment [41]. This constituted the largest category of the identified maritime cybersecurity-related studies. In this category, we also included those approaches that employed penetration testing results for the cyber security risk assessment, so there is an overlap between the studies in this category and the others and the MECE principle was not fully followed. This was implemented for those studies, whose main research contribution was in the area of risk assessment, rather than penetration testing. To be consistent, these studies were called as combinatory.
2 Design – Studies suggesting technical solutions for deterrence, identification, prevention and mitigation of the cyberattacks in the maritime ecosystem and maritime systems. This also constituted an important category of studies in maritime cybersecurity as can be observed from Fig. 8.
3 Review studies – studies providing an overview of the known ship vulnerabilities, potential attack scenarios, available regulations, methods, studies and cybersecurity issues based on the reported literature. This category of studies also attracted significant attention from researchers. The review studies were described in the introduction section of this article to justify the novelty of the present study and therefore the discussion with respect to this category of studies was not repeated herein. The findings from these studies were still used as input for the identification of research directions and challenges in the other study categories (RQ3) as well as for bibliometric analysis in RQ1. Studies which concentrated on identification of vulnerabilities and control measures lists, although constitute a valuable input to the risk assessment studies were not included in the relevant category. This was due to the fact that no formal cybersecurity assessment/analysis method was applied there.
4 Penetration testing studies – Studies demonstrating the penetration testing techniques and vulnerability scanning applied to the maritime systems. Also, some studies related to the management of testing procedures were included herein. Although input from penetration testing can be used to the risk assessment studies, since penetration testing is a different process according to NIST [44], we assigned it to a different category.
5 Cybersecurity framework – Studies focusing on cybersecurity risk management, therefore investigating more the enhancement of cybersecurity management processes and the relevant regulations and standards.
6 Maritime law – Studies investigating the impact of cyberattacks on maritime law and relevant insurance and liabilities aspects.
7 Survey studies – Studies conducting questionnaire surveys of maritime practitioners such as management personnel, seafarers, policymakers, etc. on the issues related to maritime cybersecurity.
8 Training development for cybersecurity studies – Studies aiming at the development of efficient training frameworks for maritime personnel such as seafarers or ship operators.

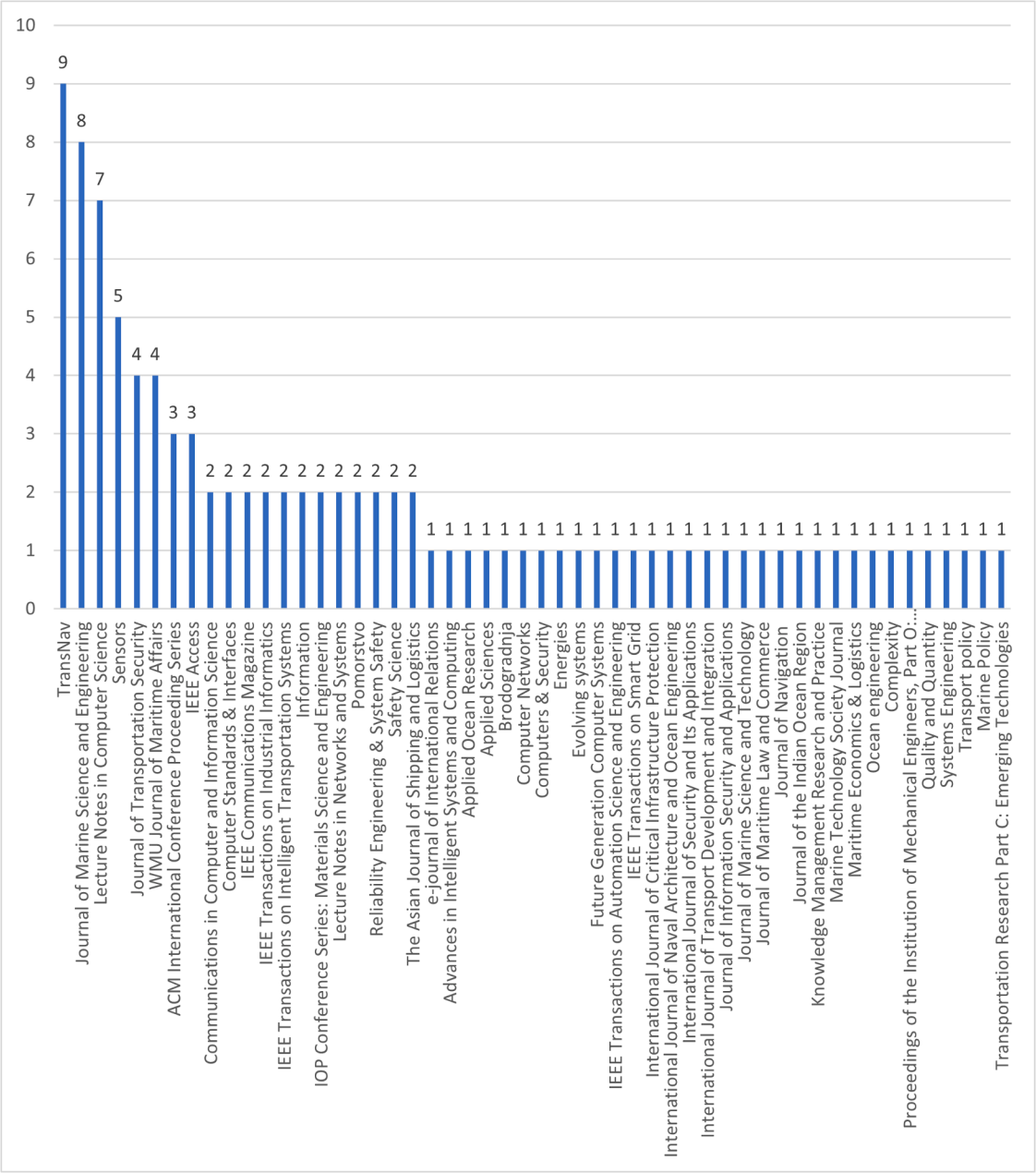

Fig. 4. The journals with the most articles related to maritime cybersecurity.

9 Cyber incidents analysis studies or cyber forensics studies – Studies identifying and analysing the causes of previously reported cybersecurity breaches or successful cyberattacks on the maritime systems as per definition in [46, 49, 50].

10 Cyber resilience studies – Studies investigating the resilience aspects of maritime cybersecurity as per definition in [47].

The employed categorisation correlated quite well with the terms identified and described in Fig. 7. It can be observed that the terms such as cyber risk assessment, management and framework were quite frequently repeated in the reported studies, indicating that separate categories should be dedicated to them. Also, term such as intrusion detection system, which is a part of technical solutions was frequently reported in the previous studies.

The research studies are analysed in more detail in the next sections of this article.

Cyber risk assessment and treatment studies

A plethora of methods were reported to be in use for cybersecurity risk assessment and cyber risk treatment in the maritime industry. An overview of the used so far methods in Scopus indexed publications is provided in Fig. 9 and the relevant studies are briefly presented in the next paragraphs. We separated the studies into those which use some type of executable, mathematical or formal model for cybersecurity risk assessment (model-based) and the one that are more dependent on manual analysis. Such as separation is frequently implemented for safety assessment methods as in [51]. The studies dependent more on manual analysis were classified further into those which incorporated safety and security analyses in line with work presented in [48] and the one which focused only on security aspects. Studies which were interlinked to several categories as elaborated in section 3.2.1 were assigned a special group.

Some of the reported studies combined the existing hazard analysis techniques with other techniques coming from the area of cybersecurity

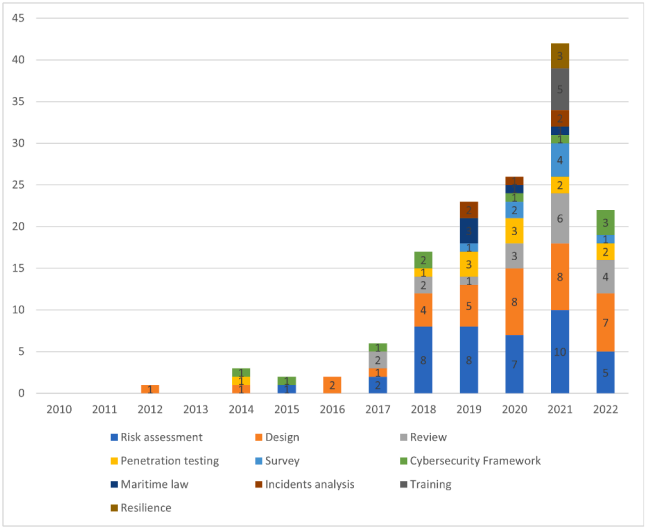

Fig. 5. The analysis of historical trends.

or computer science to implement joint analysis of safety and cybersecurity hazards/threats. Most of such studies concentrated on remotely controlled, crewless and autonomous ships. From the hazard analysis techniques, the use of System-Theoretic Process Analysis (STPA) [52] was reported frequently. In the research of Dghaym, et al. [53], STPA was combined with Event-B modelling language for cybersecurity analysis of a crewless ship. Zhou, et al. [54] used STPA to identify insecure control actions for a remotely controlled ship. Glomsrud, et al. [55] used STPA together with attack trees to identify how cyberattacks might result in unsafe control actions and hazards in an autonomous ship. Omitola, et al. [56], Cardellicchio [57] considered the use of STPA for safety and security analysis of navigational aspects in autonomous ships.

In other studies, other methods were used as a basis for joint analysis of safety and cybersecurity hazards/threats. The use of Hazard Identification (HAZID) and its modifications for cybersecurity risk assessment of a crewless inland waterway ship was reported in [58–60]. Amro, et al. [61] used the six-step model for cybersecurity and safety analysis of a small autonomous passenger ship. Vicenzutti, et al. [62] combined Fault Tree Analysis (FTA) with some identified cybersecurity scenarios for modelling threats in a ship propulsion system. Recently, a research study employing Failure Modes, Vulnerabilities and Effects Analysis (FMVEA) was conducted for identification of cyber risks in marine dual-fuel engine[63].

Some other studies focused on the elicitation of purely cybersecurity requirements in the maritime systems based on the cybersecurity risk analysis and other methods. Kavallieratos, et al. [64] identified some cyberattacks on an autonomous ship using Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege (STRIDE). In another study, Kavallieratos, et al. [65] used Secure Tropos to identify the cybersecurity requirements in an autonomous and remotely controlled ship. Meland, et al. [66] used a customized version of the Open Web Application Security Project (OWASPR) [67] to support the identification and ranking of the threat scenarios in maritime systems where little historical data was available. Jo, et al. [68] used the MITRE ATT&CK database for the identification of cyberattacks in ship systems. Similarly, de Peralta [69, 70] used the MITRE ATT&CK database for the identification of cyber threats in marine renewable systems in combination with guidance from the National

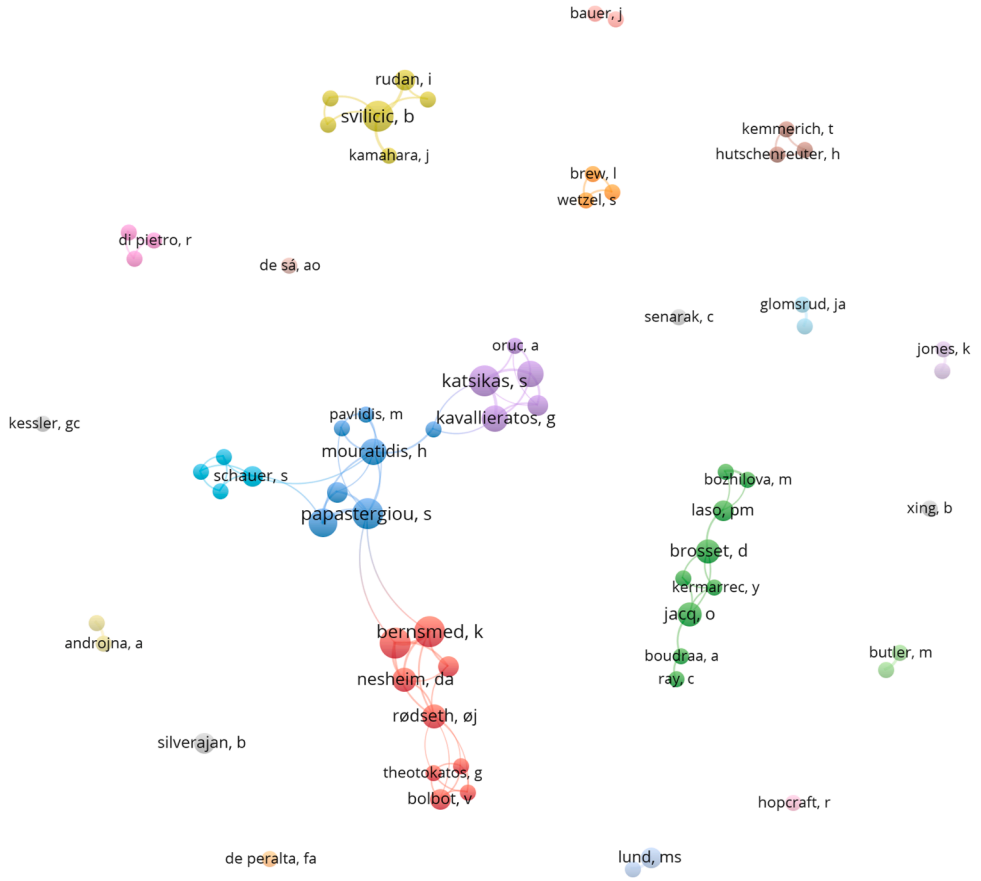

Fig. 6. Co-authorship analysis using fractional counting method, viewing authors with at least 2 papers (61 out of 422).

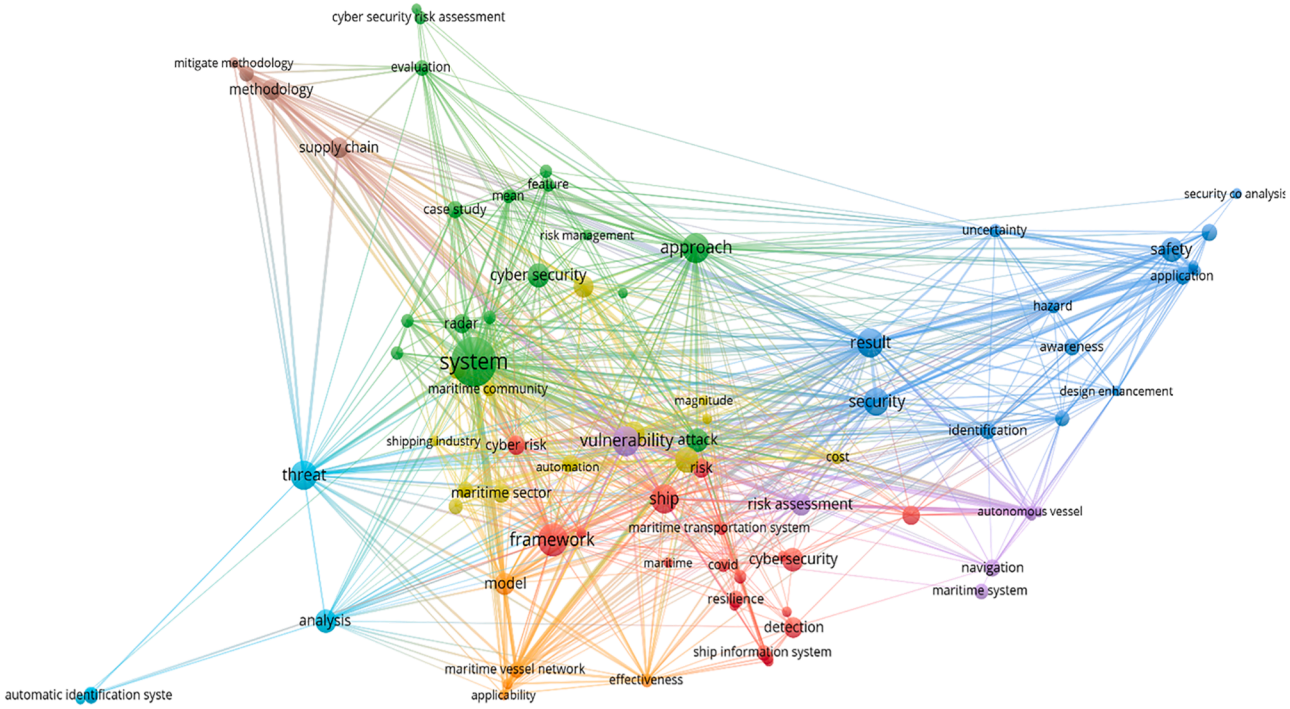

Fig. 7. Term analysis map using full counting method, including 89 out of 771 keywords.

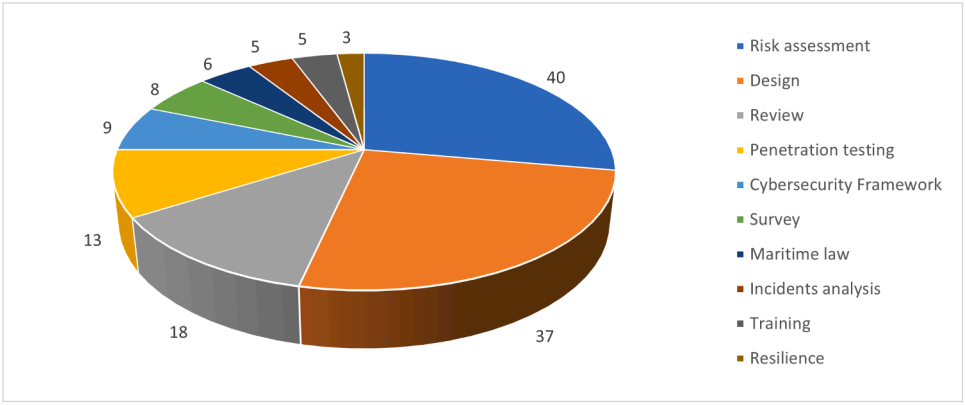

Fig. 8. Categories of research studies related to maritime cybersecurity.

Institute of Standards and Technology (NIST) [40]. Yoo and Park [71] employed a questionnaire and Analytical Hierarchical Process (AHP) to support the ranking and prioritization of cyber risk sources for cybersecurity risk management. Gunes, et al. [72] employed the Integrated Cyber Security Risk Assessment (ICSRA) model for the risk assessment of port elements. Paul, et al. [73] presented the application of Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) [74]based customized tool Oberisk for risk assessment of maritime systems. Kessler, et al. [75] suggested the use of Parkerian hexads [76] and specialised taxonomy for risk assessment of marine systems with application to AIS ship system.

Other approaches for the risk assessment involved modelling techniques for cybersecurity analysis. Weaver, et al. [77] employed an adjacency matrix to model the dependencies between the different elements of a port and used Nearly-Orthogonal Latin Hypercube and Dynamic Discretization Discovery algorithm to identify the impact of various cyberattacks considering the dependencies. Enoch, et al. [78] developed a graph-based security model which incorporated the interactions between systems on a higher level and between vulnerabilities using attack trees on a lower level to understand the effect of connections on the cybersecurity of ship systems. Another graph-based approach for risk assessment of autonomous and remotely controlled ships was proposed in [79], where DREAD (Damage, Reproducibility, Exploitability, Affected users, Discoverability) and STRIDE [80] together with interconnected nodes supported the implementation of an automatic risk assessment along with an allocation of risk control measures. Attack graphs were used to automatically identify the attack paths to maritime supply chain elements in [81]. In [82–86] a six-step approach MITIGATE (Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrAstrucTurEs) compliant with International Standard Organisation (ISO) standards for cyber-risk assessment of maritime supply chain was proposed, where dependencies were modelled using graphs.

Carreras Guzman, et al. [87, 88] proposed integrating the STPA control structure with multilayer thinking and flow of information diagrams developing a master model for an autonomous ship and subsequent cybersecurity analysis. Tam and Jones [7] proposed a distinct

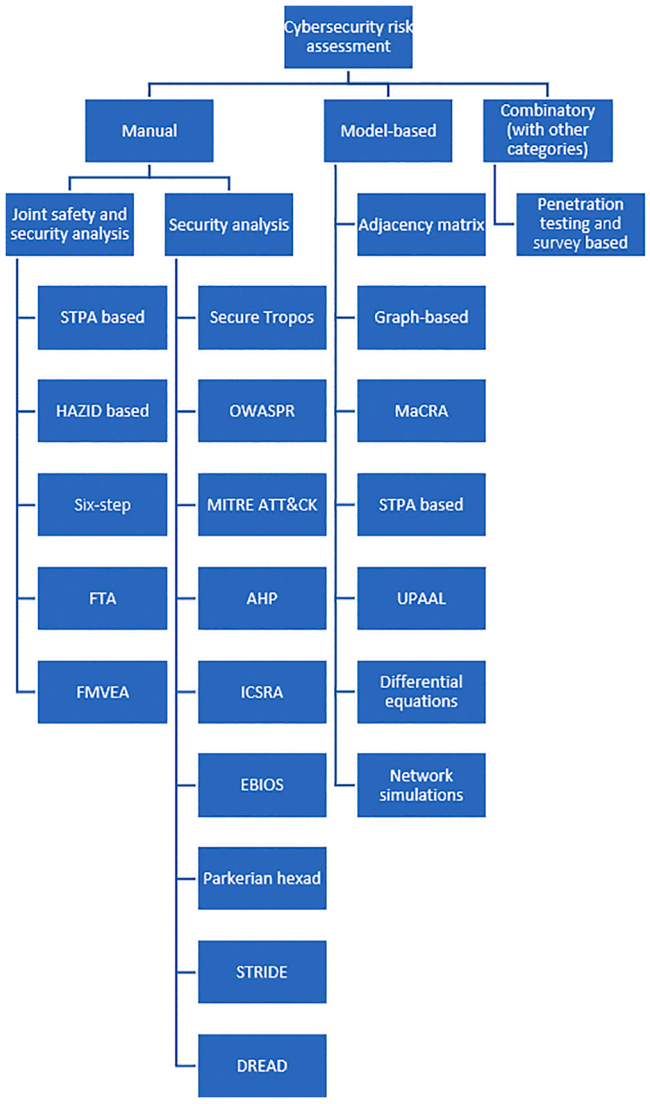

Fig. 9. The identified cybersecurity risk analysis methods.

approach named MaCRA (MAritime Cyber Risk Analysis model) where the mapping between effects, systems and technologies was used as a basis for systems and attacks ranking. Laso, et al. [89] investigated the use of role access control models to identify unauthorized access to remotely controlled ships due to the improper access models. The use of Secure Tropos for modelling and risk assessment was suggested for maritime IoT modelling in [90]. Bou-Harb, et al. [91] investigated the use of UPAAL model checker for the simulation of distributed Denial of Service attacks in marine transportation. Hassani, et al. [92] developed ship manoeuvrability models to assess the impact of Global Positioning System (GPS) spoofing attack. Penera and Chasaki [93] exploited simulations for the investigation of cyberattacks in Ethernet cables, which are widely used in ship networks.

An independent research approach for maritime cybersecurity risk assessment was demonstrated in [94–96]. In this approach, the results from a survey and penetration testing were used to support the ranking of various cyberattack scenarios. In this way, the risk assessment became evidence based.

In conclusion, it was deduced that the joint cybersecurity and safety analysis methods were quite widespread in the context of autonomous and remotely controlled ships, especially the one combining STPA with other methods. Also, an adaptation of the cybersecurity methods from other industries for cyber risk assessment of maritime systems was reported. Extensive use of graph-based risk assessment techniques from the research studies by multiple researchers was observed, whilst some of the researchers used combinatory approaches to the cyber risk assessment.

Design – technical solutions for cybersecurity development

An overview of various research studies focusing on the design of cybersecurity technical risk control measures is provided in Fig. 10. The relevant studies are briefly presented in the next paragraphs. We split these studies into the ones focusing on the design of intrusion detection systems, studies related to the design of systems supporting the visualisation and monitoring of cyber-attacks on the distributed maritime network, studies aiming at enhancing the confidentiality of ship communication through cryptography. The remaining studies were classified under another category.

One of the most frequently encountered published systems that were designed for the control of cybersecurity attack scenarios in the maritime are the intrusion detection systems (Fig. 10). The identified Scopus-indexed studies are referred to below. Liu, et al. [97] developed an intrusion detection system, which can be used to identify problems in communication systems amongst ships addressing the lack of data problem. Amro, et al. [98] proposed a systematic approach for the design of intrusion detection systems with a focus on NMEA networks considering cause-effect analysis. Gyamfi, et al. [99] used a machine learning-based intrusion detection system, which learns as new attacks appear. Nissov, et al. [100] exploited behaviour relations for the development of intrusion detection systems in a marine navigation system based on signal analysis. Boudehenn, et al. [101] proposed machine learning techniques for the development of concept intrusion detection systems for the identification of attacks in a ship communication network such as GPS spoofing attacks. Çakmakçı, et al. [102] developed an intrusion detection framework for the identification of Distributed Denial of Service attacks using formal language. Leite Junior, et al. [103] designed an intrusion detection system, which compared the known threat scenarios and the observed radar images to identify cybersecurity attacks on ships' radar or AIS. Pelissero, et al. [104] exploited graph modelling to support the identification of attacks. Iphar, et al. [105] proposed the use of an expert-designed rule-based system for the detection of spoofing attacks in AIS data. Jakovlev, et al. [106] suggested the use of simulators and statistical analysis for the detection of AIS attacks. Marcos, et al. [107] developed a system that by using statistical metrics can identify maritime GPS signal disturbances. Alincourt, et al. [108] used signal analysis and comparison with historical data for detecting the AIS attacks. Babineau, et al. [109] proposed a simple voting mechanism for the detection of attacks in a ship communication system. Onishchenko, et al. [110] proposed a detection algorithm based on the identification of "dangerous" keywords in communication messages.

Some of the studies investigated how to monitor cyberattacks in maritime ecosystem or maritime supply chain (Fig. 10). Laso, et al. [111] proposed a general framework for monitoring cyberattacks in the cruise ship industry by employing data fusion techniques. Zhao and Silverajan [112] presented a visualization platform for monitoring cyber-attacks' spread and locations by considering various stakeholders under the context of remote pilotage. An XML-based automatic cyber incidents reporting system was developed by Silverajan and Vistiaho [113] tailored to the needs of maritime. Jacq, et al. [114, 115] proposed a concept system for monitoring cyber-attacks on military ships. Pitropakis, et al. [116] developed a framework for threat detection and analysis in the maritime ecosystem with application to the Liquefied Natural Gas carrier. It can be observed that many of the studies proposed conceptual frameworks for cyberattack monitoring and not actual solutions.

A set of other studies focused on encrypting the ship communications (Fig. 10). Hemminghaus, et al. [117] proposed an encrypted communication channel for nautical communication on ships using asymmetric

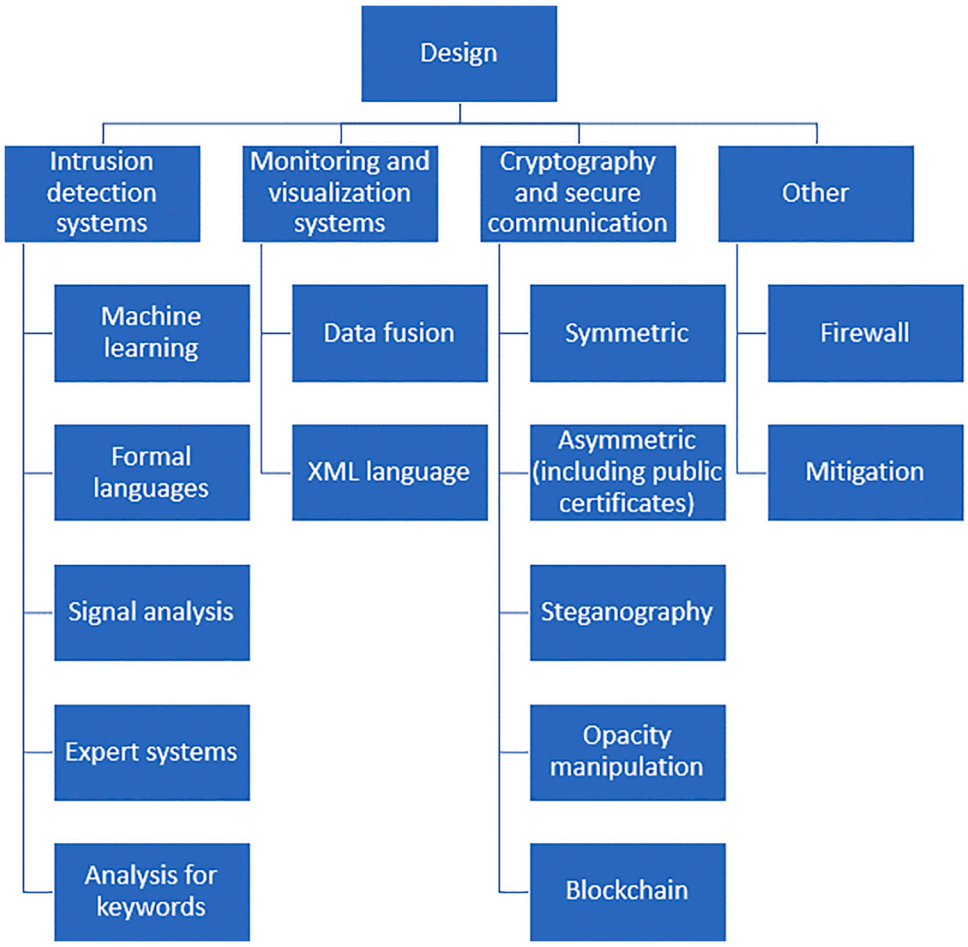

Fig. 10. The design-orientated research studies.

cryptography algorithms. Struck and Stoppe [118] proposed to encrypt AIS messages using pairing-based elliptic curve cryptography. Song, et al. [119] used a recursive watermark method for hardening a ship propulsion communication. Similarly for AIS, Aziz, et al. [120] suggested the use of elliptic curve Qu-Vanstone and elliptic curve Diffie Hellman certification schemes for encrypting the communication. Goudossis and Katsikas [121] proposed the use of public key symmetric cryptography for AIS data. Wimpenny, et al. [122] investigated the use of Public Key Cryptography for low bandwidth Very High-Frequency communications based on elliptic curve schemes. Xing, et al. [123] obscured the cyberattacks by manipulating messages opacity. Wiseman [124] proposed the use of steganography for encrypting the messages in the port's ecosystem. As it can be observed most of the encryption developments concentrated on AIS communication systems and communication algorithms.

Several studies proposed enhancement of ship secure communication through communication certificates based on asymmetric cryptography (Fig. 10) and blockchain. The development of communication certificates was often accompanied by relevant cryptographic algorithms testing [118]. Wang, et al. [125] suggested the use of blockchain for autonomous ships' communication. Grigoriadis, et al. [126] presented a series of solutions for improving maritime cybersecurity, including the novel secure communication algorithms based on SHA256 and public infrastructure certificates. Similar concepts related to public communication certificates were presented in [127–129], where different certificate types were analysed and discussed. Freire, et al. [130] proposed the use of blockchain in the maritime cybersecurity monitoring system.

In the last category (Fig. 10), a firewall for enforcing communication policy on ship networks was developed by [131]. A cyberattack fighting system in ship propulsion was proposed in [132], which was developed with the support of simulation and heuristic defence algorithms.

Concluding it can be observed that most of the encryption algorithms development effort was so far absorbed by the AIS. Also, it can be noted that the development of intrusion detection and monitoring systems received strong attention from the researchers. The development of public certificates based on asymmetric cryptography is another area of intensive research. Many of the proposed design solutions yet remained at conceptual level.

Penetration testing and vulnerability scanning studies

The penetration testing and vulnerability scanning studies were rather limited in number compared to the previously considered research study categories. This probably can be attributed to the fact that due to commercial interests and the sensitivity of the issue; the researchers were reluctant to publish their findings. The identified studies are analysed below.

Yi and Kim [133] developed guidance and framework for software security testing aligned with V design approach. Amro and Gkioulos [134] proposed a general testbed with its components for testing the maritime systems. Hemminghaus, et al. [135] developed a virtual model of an integrated bridge system, which allowed the detection of vulnerabilities and validation of cyber defences. Eichenhofer, et al. [136] demonstrated the results of vulnerability scanning in a container terminal software system using a dedicated software tool. Croteau, et al. [137] conducted penetration testing in ship systems using real equipment. Svilicic, et al. [138, 139-141] employed an industrial tool for identifying critical vulnerabilities in the ECDIS and radar systems.

Hareide, et al. [142] presented a practical example of installing and detecting malware on ECDIS during a realistic exercise. Balduzzi, et al. [143] conducted a real experiment with spoofing AIS system using specially dedicated equipment. Khandker, et al. [144] investigated the impact of various cyberattack scenarios on the AIS performance using simulations. Lee, et al. [145] employed the Model-View-View-Model design pattern for simulating naval systems and conducting the testing.

Survey studies

The survey studies mostly focused on aspects related to cybersecurity awareness as is demonstrated below. This study category is generally not so resource intensive but require access to the participants and proper questions selection and design to be successful.

Pavlinović, et al. [146] used a questionnaire to determine the cyber-awareness of the Croatian seafarers. Karamperidis, et al. [147] surveyed the perspectives of various stakeholders concerning maritime cybersecurity. Knight and Sadok [148] investigated the cybersecurity perception and readiness amongst cruise ship companies. Senarak [149, 150] investigated the required cybersecurity knowledge and skills for port facility security officers of international seaports using a survey. Heering [151] surveyed the cybersecurity awareness and management in shipping companies in Estonia. Alcaide and Llave [152] used an online questionnaire to explore the level of knowledge and training required in the general marine ecosystem. Lee and Wogan [153] investigated the preparedness and perception of cyber threats in the maritime industry.

Cybersecurity frameworks and management studies

Several studies investigated the aspects related to cybersecurity regulatory frameworks and cybersecurity management. They employed either existing standards or the existing maritime guidance as the basis for their analysis.

Lim, et al. [154] proposed a strategy for cybersecure management of big data in the maritime based on information in several cybersecurity standards. In [9] a systemic approach to the management of cybersecurity in a ship operating company was presented. Drazovich, et al. [155] proposed updates in the regulatory framework based on the review of existing maritime guidance. Pappalardo, et al. [156] developed a framework for cybersecurity management based on the comparison between risk management frameworks in different transportation sectors. Hopcraft and Martin [157] elaborated the principles for a detailed maritime cybersecurity code. Trimble, et al. [158] identified the main risk factors and proposed an independent public entity for assessing, containing, and mitigating cyber risks in the maritime. Bernsmed, et al. [159] demonstrated how the cyber-risks can be depicted on the Bow-Tie and how the classical Bow-Tie can be used to support risk management using a ship communication system as example. Papastergiou, et al. [160], Papastergiou and Polemi [161] presented an innovative physical/cyber security management system for ports and principles for cyber security risk management.

Maritime law and insurance framework studies

The intersection between maritime law, liabilities, insurance, and cybersecurity received little research attention despite its importance in Scopus-indexed publications. The few identified studies are demonstrated below.

Al Ali, et al. [162] reviewed the legal basis for cybersecurity in maritime transportation and various legal acts. de Faria [163] recommended a new legal code based on the analysis of existing regulations for maritime cybersecurity and some legal principles. Greiman [164] analysed the maritime security laws and investigated the shipowners' liability principles and national and maritime strategies in connection to maritime cybersecurity. Ramluckan [165] investigated the applicability of the Tallinn manuals to the problems related the maritime cybersecurity in the South Africa region. Daum [166] reviewed the international law in connection to maritime cyberattacks based on factual circumstances and cyber-attack cases.

Training development studies

The number of research studies on training framework development is also limited in number. As described below though, the use of simulators for the training of maritime personnel becomes more popular.

Hopcraft [167] proposed integration between the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers and NIST frameworks to develop a set of requirements for seafarers training. Potamos, et al. [168] proposed a training framework employing cyber range as a basis for development. Jacq, et al. [169] considered the use of cyber simulations for personnel training. Kuhn, et al. [170] conducted a training exercise in the case of a cyber-attack on a maritime system. Shapo and Levinskyi [171] investigated the aimed skills and the equipment necessary for seafarers' training in maritime cybersecurity.

Cyber incidents analysis studies

The number of studies investigating previous cyber incident analysis was also limited. This can be attributed to the fact that the ship operating companies avoid reporting cyber incidents to avoid negative publicity [5, 8], therefore the available input information can be scarce.

Androjna, et al. [172], Androjna, et al. [173] investigated a case of AIS spoofing on a ship. In [5] 49 maritime cyber incidents were analysed to identify the intensity and aims of cyberattacks. Awan and Al Ghamdi [174] investigated 59 safety and cybersecurity incidents concerning the ship systems components to identify vulnerabilities and potential cyber-attacks. Tam and Jones [175] examined the maritime industry readiness for implementation of systematic cyber incidents investigation and provided recommendations for relevant process enhancement and application.

Cyber resilience studies

Cyber resilience in maritime received even less attention than the previous studies categories in terms of Scopus-indexed publications. This can be attributed partially to the fact that some of the resilience aspects were discussed in the papers on training program development and partially to the fact that this issue is still arising. It is a noteworthy area as the ability to respond to unanticipated cyber-attacks is of high importance [176].

Brew, Drazovich and Wetzel [2] investigated the impact of COVID-19 on the resilience of maritime supply chains in the view of an increased potential for cyber-attacks. Hutschenreuter, et al. [177] proposed an ontology for the development of relevant cybersecurity and resilience framework. Erstad, Ostnes and Lund [176] provided a working definition of maritime cybersecurity resilience based on the analysis of relevant terminology and relevant incidents.

RQ3: The methodological challenges and research directions and topics in connection to the maritime cybersecurity

Based on the investigated papers several challenges and research directions and topics were identified. They are presented in Table 1.

Table 1
Methodological challenges, research directions and topics based on the literature.

Challenges	Research directions and topics
Cybersecurity risk assessment	
1. The difficulty with accurate prioritization of cyberattack scenarios due to the lack of accurate historical cyber incidents information to support credible cyber risk assessments [7, 66], the cost of having a diverse group of experts in risk assessments [59, 66], unknown interactions between systems and risk factors [21, 71, 77], constantly evolving nature of the area considering the long lifecycle ships [15, 58] and diversity of marine equipment suppliers [15]. 2. Secondarily, the transferability of results of one risk assessment needs to be ensured [66]. 3. Having efficient, not resource-intensive risk assessment is another challenge [66, 78]. 4. Ensuring sufficient communication amongst various stakeholders during risk assessment can be a challenge [20, 59, 73]. 5. It can also be challenging to identify the effects of connectivity and complex cyberattacks as it is challenging to accurately represent the operational and information technologies in ships and the relevant temporal and functional relationships [4, 78, 79, 81, 84]. 6. The lack of efficient cybersecurity metrics constitutes another challenge [78]. 7. Model-based approaches require significant computational power for their application [77] associated with state-space growth [61]. 8. Lack of credible and commonly agreed risk acceptance criteria for cyber risk is another area of concern [15, 26, 58, 59]. 9. The selection of appropriate scales for risk ranking can be a challenge [105].	1. Threat and security requirements analysis for communication protocols used in maritime [16, 68]. 2. Implementation of comparative studies between the different cyber risk assessment techniques. 3. Use of novel joint safety and cybersecurity assurance techniques [18, 19, 29, 48, 61]. 4. Integration of various cybersecurity methods [53]. 5. Development of novel ontologies for representation of ship systems in cybersecurity risk assessment [78, 87]. 6. Alignment of cyber risk assessment processes with standards and standardization of risk assessment approaches [59, 71]. 7. Development of widely recognized cyber risk acceptance criteria in maritime [59]. 8. Investigation of interrelationships between maritime cybersecurity, trust, and technology acceptance. 9. Research on collaborative and multiple cyberattacks is required [78]. 10. Development of efficient cybersecurity risk assessment and risk monitoring key performance and metrics [78, 91, 156]. 11. Further advancement of model-based tools for cyber security risk assessment with application to maritime systems [178]. 12. Use of game-based risk assessment approaches [90]. 13. Development of cybersecurity risk assessment tools together with optimization tools and other design tools [79]. 14. Implementation of cybersecurity studies in maritime considering human factors and interactions with autonomous systems [87]. 15. Interconnection of risk assessment techniques with machine learning techniques for automatic cybersecurity analysis [81]. 16. Development of automatic techniques for identifying improper access management settings [89]. 17. More studies related to the perception of cyber risk are required [17]. 18. More risk assessment studies in connection with novel maritime systems such as remote control centre can be implemented [14, 23]. 19. Investigation of trade-off between cybersecurity and efficiency [63]. 20. Holistic optimisation studies of maritime systems considering efficiency, safety, costs and cybersecurity.
Design – technical solutions for cybersecurity development	
10. Increased demand for communication bandwidth and computational power for ensuring secure transmissions or reporting of incidents [75, 113, 120, 128, 130, 179] which might render challenging the development of wide-scale monitoring systems [130]. 11. Integration of information from multiple stakeholders in intrusion detection systems can be a challenging task [116] due to difficulty with timely model parameters aggregation [97]. 12. Increased computational demand for the operation of intrusion detection systems [99]. 13. Problems with increased latency due to encryption [117] or increased computational cost [130]or needs for additional authentication[179] can arise. 14. Difficulty with discriminating different risks and attack types [105] in intrusion detection systems. This includes difficulty with the identification of advanced attack types and confusion with physical failures [98]. For that, a thorough understanding of systems and input data for solutions developments is required [105]. 15. Network instabilities dishearten the establishment of secure communications and authenticity protocols [118, 125, 128, 179]. 16. Challenges with services integration [126]. 17. The international nature of maritime shipping complicates the development of commonly agreed public communication certificates [128]. 18. The wide availability of AIS equipment vendors renders the adaptation of singular cybersecure communication protocol challenging [121]. 19. Technical challenges can arise during revocation or reissue of public keys [121]. 20. Issues related to the physical protection of storage systems for public certificates need to be resolved [129].	21. Development of honeypot systems in the maritime for collecting information about the threat behaviour and actors [68]. 22. Automatic cyberattack identification, monitoring, and response systems development [23, 58, 68, 69, 71, 101, 111, 169]. 23. Development of novel ontologies for the previously mentioned systems [102, 177]. 24. Development of flow whitelist management systems in the maritime [68]. 25. Development of real-time risk assessment tools for cybersecurity [21, 84, 90, 111, 126]. 26. Novel transmission authentication techniques including wired protocols [23, 75]. 27. Use of filtering techniques for spoofing identification [75]. 28. Use of predictive communication techniques [75]. 29. Software hardening techniques development [126] 30. Development of trust estimation-based communication systems considering network instabilities and time factors [118, 125, 126]. 31. Development of novel secure and efficient communication algorithms [124, 126] 32. Development of solutions on higher Technology Readiness Level [117, 168]. 33. Development of novel, widely acceptable public certificate types [128, 179]. 34. Validation studies for user-friendliness of the developed solutions and better consideration of human factors during the design of the solutions [105]. 35. Various monitoring systems integration [114]. 36. Standardisation of communication protocols [23] 37. Fusing artificial intelligence and blockchain capabilities [130].
Penetration testing and vulnerability scanning studies	
21. The implementation of thorough penetration testing is challenging as the list of known vulnerabilities is constantly updated, which needs to be reflected in the penetration testing tools [58]. 22. Conflicts in testing between cybersecurity and functional/performance testing [133]. 23. The in-depth software assessment can be also resource-intensive [136]. 24. Ensuring transparency in vulnerability scanning can be an important challenge [136, 145] 25. Lack of regulations controlling the vulnerability scanning process [136], although there are some standards under development [138]. 26. Lack of skilful personnel [136]. 27. Issues with latency between the testing and visualisation [134]	38. Development of novel penetration testing and vulnerability scanning techniques, which are interconnected with remotely updated databases [103]. 39. Development of remote penetration testing techniques. 40. Development of testing techniques for components with learning capacity and considering users' behaviour [134]. 41. Integration of penetration testing with ship cybersecurity design and management processes [133, 134]. 42. Automatization of the testing process and use of purple teaming [134]. 43. Testing techniques development for novel technical systems and solutions [112]

(*continued on next page*)

Table 1 (*continued*)

Challenges	Research directions and topics
Cybersecurity risk assessment	
28. Challenges with the testbed mobility, scalability and integration into the design and management process [134]. 29. The heterogeneity of systems to be modelled to allow effective simulations of cyberattacks [144].	
Survey studies	
30. The limited number of professionals [148]. 31. The maritime practitioners might be very conservative and restrained in their responses [151].	44. Survey on wider public opinions related to maritime cybersecurity and on how this influences trust. 45. Investigation of other stakeholders' readiness and perspectives on maritime cybersecurity [148, 150] using advanced statistical tools [147]. 46. Survey of interrelationships between cybersecurity, autonomous ships and public perspectives. 47. Survey of cyber awareness in a wide number of countries in a periodical manner [151].
Cybersecurity frameworks and management studies	
32. The increased window of opportunities and constant evolution of the cyber threats [18, 58]. 33. Fragmentation in the regulations [20, 22]. 34. Lack of cyber incidents monitoring entity [158]. 35. A large lifetime of ships extending up to 25 years [9]. 36. A large variety of involved stakeholders [9]. 37. Low cybersecurity awareness[9]. 38. The impact of COVID-19 [9] 39. The heterogeneity of maritime equipment suppliers [15]. 40. As it is also believed by some researchers, the current maritime cyber security regulations are not grounded in research, do not address the aspects holistically, refer to industry agnostic guidelines and are lagging behind the research developments [155, 157].	48. Development of tools allowing traceability of cybersecurity requirements and integration between requirements and systems with a focus on the maritime systems [53, 180]. 49. Development of novel efficient tools for risk communication [73]. 50. Development of tools for constant update of vulnerabilities databases [7]. 51. Use of tools for constant access management [89] and efficient audit of maritime systems[19]. 52. Enhancement of cyber risk management processes and tools[160]. 53. Standardisation of approaches for cyber risk management [22]. 54. Investigation of interactions between technical cybersecurity and business topics management. 55. Research on cybersecure management of big data in maritime[154].
Maritime law and insurance framework studies	
41. As for maritime regulations, due to the international character of shipping industry, any legislative developments are inhibited[162, 163, 165]. 42. The development of legislative tools is also inhibited due to the fragmentation in the legislative frameworks [164]. 43. The lack of awareness, complexity and interdependency between stakeholders [22] 44. The lack of regulations and laws enforcement entity [181]. 45. The lack of specificity [181].	56. More high quality collaborative research in the area is required to develop legislative measures[162, 181] by ensuring clarity and promoting uniform application and deterrent punishment[181].
Training development studies	
46. The lack of standardization in the required competencies [20, 167] 47. Constant development of new cyber-attack types [167, 170].	57. Development of training schemes for cyber incident reporting [175]. 58. Increasing awareness of cybersecurity vulnerabilities in the maritime community [7, 25, 68, 71]. 59. Training on ensuring mitigation and resilience in cyberattacks and general management of cyberattacks [20, 25, 152, 167]. 60. Training development for use of formal methods [53]. 61. Use of simulations for the training of maritime personnel [12, 168, 169]. 62. Rehearsal of the minimum set of digital skills for seafarers and maritime practitioners [167, 168]. 63. Development of performance measurement metrics for training[170]
Cyber incidents analysis studies	
48. Lack of complete information about the cyber incidents [175]. 49. Lack of relevant regulatory framework [69, 175]. 50. Technical limitations for data aggregation [175]. 51. Difficulty of classifying the cyber-attack into major or minor as the consequence can be not visible at the moment of occurrence [20].	64. Development of a regulatory framework for cyber-incidents reporting [69]. 65. Development of forensic technology for automatic incidents analysis [68, 175]. 66. Development of advanced classification for incidents reporting [113, 175]. 67. Development of comprehensive methodology for cyber incidents analysis similarly to the accident investigation methods. 68. Development of information platforms for sharing experiences about cybersecurity incidents [5]. 69. Development of novel incidents reporting formats [113, 114]. 70. Development of processes for cyber incidents investigation management [175].
Cyber resilience studies	
52. The lack of standardization in emergency response plans [20].	71. Development of emergency procedures management including training for addressing unexpected cyber events [18, 26]. 72. Development of model-based approaches for cyber security resilience [177]. 73. More empirical studies on maritime cyber-resilience are required [177].

Limitations to the review process

One of the limitations of this study is the use of Scopus as the search engine, which may have resulted in the exclusion of some scientific publications with significant contributions. However, Scopus can be deemed as a credible search engine and the number of publications that were considered in this review is significant. In addition, the number of research directions and topics identified in this article is substantial and this is indicative of the breadth and depth of the conducted analysis.

The review and research investigation focused primarily on academic publications. White papers or industrial perspectives and research initiatives, as well as governmental and regulatory documents, were not included. The research conducted by the navies in naval cybersecurity is an important area in maritime cybersecurity. However, most of the results are highly classified and not accessible for general readers. Some of the work from the navy that appeared in Scopus was included in the analysis. Still, it is hoped that some of the best practises and methodologies identified in this article would be of interest to all stakeholders, including navies and industries.

Conclusions

In this article, a systematic literature review and bibliometric analysis of the available research studies in Scopus on maritime cybersecurity were implemented. The bibliometric analysis helped to identify the leading countries, the most prevalent journals, researchers, and their cooperation links, as well as historical trends in maritime cybersecurity (RQ1). The literature review further identified the categories of research studies and the methodologies employed so far for maritime studies (RQ2). An analysis of the investigated papers also resulted in the identification of research challenges and directions for future research (RQ3). In this way, this article provides a succinct summary of the advancements in maritime cybersecurity through academic publications.

The main findings of this study are as follows:

- Norway, the United Kingdom (UK), France and the USA had the highest contributions, based on the number of Scopus indexed publications. Europe leads the field when considering authors with two or more articles.
- Journal of Marine Science and Engineering and TransNav were found to have the highest number of publications on maritime cybersecurity. Other notable journals included Lecture Notes in Computer Science, Journal of Transportation Security, Sensors, and WMU Journal of Maritime Affairs.
- The annual number of scientific publications on maritime cybersecurity is consistently on the rise. The research topics' diversity and employed methodologies have also increased since 2017.
- Joint publications amongst two or more research groups are not common, with most of the articles coming from within individual research groups.
- The topics of concern for maritime cybersecurity researchers included cyber risk and uncertainty management, risk modelling, risk evaluation, increasing cybersecurity awareness, and investigating the applicability of different methods to the maritime systems. Researchers also examined the relationship between safety and cybersecurity on ships, various attack types and the impact of COVID-19 on the industry, development of novel cybersecurity solutions and cybersecure autonomous ships.
- The most frequent research studies included cyber risk assessment and developing novel systems for cyber security control. They contributed to over 50% of the total considered studies.
- Other topics in connection to maritime cybersecurity such as penetration testing techniques, regulatory cybersecurity framework and management development, interactions between maritime law and cybersecurity, training for cybersecurity, cyber incidents analysis and cyber resilience received much less attention than the topics related to cybersecurity risk assessment and design of technical solutions.
- Based on the considered studies, 52 methodological challenges and 73 research directions in different topics were identified.

The results from the bibliometric analysis can be used by policy makers to gain insights on research groups, cooperation's and direction of research. This information may help shape the course of future investments in research. The identified and analysed research studies, methodological challenges and the proposed research directions can support conducting focused innovative research. Therefore, it is expected that this review paper will support the development of research proposals, novel methodologies and technical solutions and generally will promote maritime cybersecurity. A future review study could consider additional research questions or could focus on a more detailed analysis of any considered topic in this review paper. A more extensive review could consider including also non-Scopus indexed research studies and incorporating to greater extent industrial perspectives in the review.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data is available in Appendix A, as a part of supplementary material.

Acknowledgments

The study was carried out in the framework of AutoMare project funded by Finnish Ministry of Education and Culture under application number 117784. Constructive feedback from anonymous reviewers is also acknowledged. The opinions expressed herein are those of the authors and should not be construed to reflect the views of Finnish Ministry of Education and Culture, acknowledged individuals and other involved partners in the AutoMare project.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.ijcip.2022.100571.

References

[1] G. Aiello, et al., Towards Shipping 4.0. A preliminary gap analysis, Procedia Manuf. 42 (2020) 24–29.
[2] L. Brew, et al., The Impact of COVID-19 on the Security and Resilience of the Maritime Transportation System, in: 2021 IEEE International Conference on Cyber Security and Resilience (CSR), IEEE, 2021, pp. 510–517.
[3] Ø.J. Rødseth, et al., D4.5 Architecture specification, in, 2015.
[4] V. Bolbot, et al., Vulnerabilities and safety assurance methods in Cyber-Physical Systems: a comprehensive review, Reliab. Eng. Syst. Saf. 182 (2019) 179–193.
[5] P.H. Meland, et al., A retrospective analysis of maritime cyber security incidents, TransNav (2021) 15.
[6] F. Landon, Defence against the next level of cyber-threat, Marine Professional (2021) 7–9.
[7] K. Tam, K. Jones, MaCRA: a model-based framework for maritime cyber-risk assessment, WMU J. Maritime Affairs 18 (2019) 129–163.
[8] K. Munro, Cybersecurity and shipping: a sitting duck?, (2021) 23.
[9] E. Kechagias, et al., Digital transformation of the maritime industry: a cybersecurity systemic approach, Int. J. Critical Infras. Protection 37 (2022), 100526.
[10] L. Nate, The cost of a malware infection? For Maersk, $300 million, Digital guardian, (2020).
[11] Obrela, Security attack landscape Q2'2021 vs Q2020, in, 2021.
[12] A. Oruc, et al., Towards a Cyber-Physical Range for the Integrated Navigation System (INS), J. Mar. Sci. Eng. 10 (2022) 107.
[13] M.A. Ben Farah, et al., Cyber security in the maritime industry: a systematic survey of recent advances and future trends, Information 13 (2022) 22.
[14] H.M. Tusher, et al., Cyber security risk assessment in autonomous shipping, Maritime Econ. Logistics (2022) 1–20.
[15] I. Ashraf, et al., A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry, IEEE Trans. Intell. Transp. Syst. (2022).
[16] G.C. Kessler, The CAN Bus in the Maritime Environment–Technical Overview and Cybersecurity Vulnerabilities, TransNav 15 (2021).
[17] M.H. Larsen, M.S. Lund, A Maritime Perspective on Cyber Risk Perception: a Systematic Literature Review, IEEE Access (2021).
[18] I. de la Peña Zarzuelo, Cybersecurity in ports and maritime industry: reasons for raising awareness on this issue, Transp Policy (Oxf), 100 (2021) 1–4.
[19] I. Progoulakis, et al., Cyber Physical Systems Security for Maritime Assets, J. Mar. Sci. Eng. 9 (2021) 1384.
[20] N. Adams, et al., How port security has to evolve to address the cyber-physical security threat: lessons from the SAURON project, Int. J. Trans. Develop. Integ. 4 (2020) 29–41.
[21] N. Adams, et al., Guidance for ports: security and safety against physical, cyber and hybrid threats, J. Transport. Sec. 14 (2021) 197–225.

[22] M. Bocayuva, Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic, WMU J. Maritime Affairs 20 (2021) 173–192.
[23] M. Caprolu, et al., Vessels cybersecurity: issues, challenges, and the road ahead, IEEE Commun. Mag. 58 (2020) 90–96.
[24] G. Kavallieratos, et al., Modelling shipping 4.0: a reference architecture for the cyber-enabled ship, in: Asian Conference on Intelligent Information and Database Systems, Springer, 2020, pp. 202–217.
[25] S. Ahvenjärvi, et al., Safe information exchange on board of the ship, TransNav (2019) 13.
[26] L.R. Shapiro, et al., Trojan horse risks in the maritime transportation systems sector, J. Transp. Security 11 (2018) 65–83.
[27] B. Silverajan, et al., Cybersecurity Attacks and Defences for Unmanned Smart Ships, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 15–20.
[28] I. Botunac, M. Gržan, Analysis of software threats to the automatic identification system, Brodogradnja 68 (2017) 97–105.
[29] B. You, et al., Review on cyber security risk assessment and evaluation and their approaches on maritime transportation, in: Proceedings of the 30th Annual Conference of International Chinese Transportation Professionals Association, Houston, TX, USA, 2017, pp. 19–21.
[30] A. Liberati, et al., The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration, J. Clin. Epidemiol. 62 (2009) e1–e34.
[31] A. Booth, et al., Systematic approaches to a successful literature review, (2021).
[32] D. Moher, et al., Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement, Ann. Intern. Med. 151 (2009) 264–269.
[33] IFERP, Scopus vs Web of science journal; Which one is better, in, 2022.
[34] Scimago, Scimago Journal and Country Rank, in, 2022.
[35] VOSviewer, in, 2018.
[36] A. Perianes-Rodriguez, et al., Constructing bibliometric networks: a comparison between full and fractional counting, J. Informetr. 10 (2016) 1178–1195.
[37] V. Pareto, A. Page, Manuale Di Economia Politica (Manual of Political Economy), Societa Editrice Libraia, Milan, Italy, 1906.
[38] ISO, Risk management - Guidelines - ISO 31000, in, British Standards Institution, 2018.
[39] NIST, Risk assessment, in, 2022.
[40] NIST, Computer security resource center, in, 2019.
[41] M. Chapple, et al., ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide, John Wiley & Sons, 2018.
[42] NIST, Vulnerability assessment, in, 2022.
[43] NIST, NIST.SP.800-53rev5, in, NIST, 2022.
[44] NIST, Penetration testing, in, 2022.
[45] The Role of the Semi-Submersible Work Vessel In Offshore Production Operations, in: J.L. Arps (Ed.), Offshore Technology Conference, Houston, Texas, 1973.
[46] N. Oliviah, Cyber Incident Analysis, in, 2019.
[47] NIST, Resilience, in, 2022.
[48] S. Kriaa, et al., A survey of approaches combining safety and security for industrial control systems, Reliab. Eng. Syst. Saf. 139 (2015) 156–178.
[49] J. Vacca, Computer and Information Security Handbook, 2017.
[50] L. Daniel, L. Daniel, Digital Forensics For Legal Professionals, Digital Forensics for Legal Professionals, 2012.
[51] S. Sharvia, et al., Model-based dependability analysis: state-of-the-art, challenges, and future outlook, in: R. Soley, N. Ali, J. Grundy, B. Tekinerdogan (Eds.), Software Quality Assurance, Morgan Kaufmann, Boston, 2016, pp. 251–278.
[52] N. Leveson, J. Thomas, STPA Handbook, 2018.
[53] D. Dghaym, et al., An STPA-based formal composition framework for trustworthy autonomous maritime systems, Saf. Sci. 136 (2021), 105139.
[54] X.-.Y. Zhou, et al., A system-theoretic approach to safety and security co-analysis of autonomous ships, Ocean Eng. 222 (2021), 108569.
[55] J.A. Glomsrud, et al., A Structured STPA Safety and Security Co-analysis Framework for Autonomous Ships, in: European Safety and Reliability conference, Germany, Hannover, 2019.
[56] T. Omitola, et al., Securing navigation of unmanned maritime systems, (2018).
[57] D. Cardellicchio, Naval Automation Cyber Defence Guidelines, in: Technology and Science for the Ships of the Future, IOS Press, 2018, pp. 943–949.
[58] V. Bolbot, et al., A novel cyber-risk assessment method for ship systems, Saf. Sci. 131 (2020), 104908.
[59] V. Bolbot, et al., A novel risk assessment process: application to an autonomous inland waterways ship, in: Proceedings of the Institution of Mechanical Engineers, 2021. Part O: Journal of Risk and Reliability, 01748006×211051829.
[60] V. Bolbot, et al., Safety related cyber-attacks identification and assessment for autonomous inland ships, in: Internation Seminar on Safety and Security of Autonomous Vessels, Helsinki, Finland, 2019.
[61] A. Amro, et al., Impact of cyber risk on the safety of the MilliAmpere2 Autonomous Passenger Ship, in: IOP Conference Series: Materials Science and Engineering, IOP Publishing, 2020, 012018.
[62] A. Vicenzutti, et al., Dependability analysis of cyber security in All-Electric Ships, in: 2018 AEIT International Annual Conference, IEEE, 2018, pp. 1–5.
[63] V. Bolbot, et al., Identification of cyber-attack scenarios in a marine Dual-Fuel engine, Trends Maritime Technol. Engin. 1 (2022) 503–510.
[64] G. Kavallieratos, et al., Cyber-Attacks Against the Autonomous Ship, in: S. K. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, A. Antón, S. Gritzalis, et al. (Eds.), Computer Security, Springer International Publishing, 2019, pp. 20–36.
[65] G. Kavallieratos, et al., Shipping 4.0: security requirements for the cyber-enabled ship, IEEE Trans. Ind. Inf. 16 (2020) 6617–6625.
[66] P.H. Meland, et al., Assessing cyber threats for storyless systems, J. Inform. Secur. Appl. 64 (2022), 103050.
[67] J. Williams, OWASP risk rating methodology, in, 2020.
[68] Y. Jo, et al., Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework, Sensors 22 (2022) 1860.
[69] F.A. de Peralta, Cybersecurity Resiliency of Marine Renewable Energy Systems-Part 1: identifying Cybersecurity Vulnerabilities and Determining Risk, Mar. Technol. Soc. J. 54 (2020) 97–107.
[70] F.A. de Peralta, et al., Cybersecurity Resiliency of Marine Renewable Energy Systems Part 2: cybersecurity Best Practices and Risk Management, Mar. Technol. Soc. J. 55 (2021) 104–116.
[71] Y. Yoo, H.-.S. Park, Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans in Consideration of Digitalized Ship, J. Mar. Sci. Eng. 9 (2021) 565.
[72] B. Gunes, et al., Cyber security risk assessment for seaports: a case study of a container port, Comput. Secur. 103 (2021), 102196.
[73] S. Paul, et al., Obérisk: cybersecurity Requirements Elicitation through Agile Remote or Face-to-Face Risk Management Brainstorming Sessions, Information 12 (2021) 349.
[74] EBIOS, EBIOS Risk Manager, in: A.n.d.l.s.d.s. d'information (Ed.), Paris, France, 2019.
[75] G.C. Kessler, et al., A taxonomy framework for maritime cybersecurity: a demonstration using the automatic identification system, TransNav 12 (2018) 429.
[76] S. Controls, Toward a new framework for information security. Computer Security Handbook, 2012. Set.
[77] G.A. Weaver, et al., Estimating economic losses from cyber-attacks on shipping ports: an optimization-based approach, Transport. Res. Part C 137 (2022), 103423.
[78] S.Y. Enoch, et al., Novel security models, metrics and security assessment for maritime vessel networks, Computer Networks 189 (2021), 107934.
[79] G. Kavallieratos, et al., Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems, Sensors 21 (2021) 1691.
[80] A. Shostack, Experiences Threat Modeling at Microsoft, MODSEC@ MoDELS, 2008 (2008) 35.
[81] N. Polatidis, et al., From product recommendation to cyber-attack prediction: generating attack graphs and predicting future attacks, Evolving Syst. 11 (2020) 479–490.
[82] S. Schauer, et al., MITIGATE: a dynamic supply chain cyber risk assessment methodology, J. Transpor. Secur. 12 (2019) 1–35.
[83] E.-.M. Kalogeraki, et al., A Novel Risk Assessment Methodology for SCADA Maritime Logistics Environments, Appl. Sci. 8 (2018) 1477.
[84] N. Polatidis, et al., Cyber-attack path discovery in a dynamic supply chain maritime risk management system, Comput. Stand. Interfaces 56 (2018) 74–82.
[85] E.-.M. Kalogeraki, et al., Modeling SCADA attacks. Smart Trends in Systems, Security and Sustainability, Springer, 2018, pp. 47–55.
[86] E.-.M. Kalogeraki, et al., Knowledge management methodology for identifying threats in maritime/logistics supply chains, Knowledge management research & practice 16 (2018) 508–524.
[87] N.H. Carreras Guzman, et al., Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis, Syst. Engin. 23 (2020) 189–210.
[88] N.H.C. Guzman, et al., A Comparative Study of STPA-Extension and the UFoI-E Method for Safety and Security Co-analysis, Reliab. Eng. Syst. Saf. 211 (2021), 107633.
[89] P.M. Laso, et al., Defining role-based access control for a secure platform of unmanned surface vehicle fleets. OCEANS 2019-Marseille, IEEE, 2019, pp. 1–4.
[90] H. Mouratidis, V. Diamantopoulou, A security analysis method for industrial Internet of Things, IEEE Trans. Ind. Inf. 14 (2018) 4093–4100.
[91] E. Bou-Harb, et al., On the impact of empirical attack models targeting marine transportation, in: 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), IEEE, 2017, pp. 200–205.
[92] V. Hassani, et al., Cyber security issues in navigation systems of marine vessels from a control perspective, in: International Conference on Offshore Mechanics and Arctic Engineering, American Society of Mechanical Engineers, 2017 pp. V07BT06A029.
[93] E. Penera, D. Chasaki, Packet scheduling attacks on shipboard networked control systems. 2015 Resilience Week (RWS), IEEE, 2015, pp. 1–6.
[94] B. Svilicic, et al., A study on cyber security threats in a shipboard integrated navigational system, J. Mar. Sci. Eng. 7 (2019) 364.
[95] B. Svilicic, et al., Maritime cyber risk management: an experimental ship assessment, J. Navigation 72 (2019) 1108–1120.
[96] B. Svilicic, et al., Raising awareness on cyber security of ECDIS, TransNav 13 (2019).
[97] W. Liu, et al., Intrusion Detection for Maritime Transportation Systems With Batch Federated Aggregation, IEEE Trans. Intell. Transp. Syst. (2022).
[98] A. Amro, et al., Navigation Data Anomaly Analysis and Detection, (2022).
[99] E. Gyamfi, et al., An Adaptive Network Security System for IoT-Enabled Maritime Transportation, IEEE Trans. Intell. Transp. Syst. (2022).

[100] M.C. Nissov, et al., Analysing Cyber-resiliency of a Marine Navigation System using Behavioural Relations, in: 2021 European Control Conference (ECC), IEEE, 2021, pp. 1385–1392.
[101] C. Boudehenn, et al., Navigation anomaly detection: an added value for Maritime Cyber Situational Awareness, in: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), IEEE, 2021, pp. 1–4.
[102] S.D. Çakmakçı, et al., A Framework For Intelligent DDoS Attack Detection and Response using SIEM and Ontology, in: 2021 IEEE International Conference on Communications Workshops (ICC Workshops), IEEE, 2021, pp. 1–6.
[103] W.C. Leite Junior, et al., A triggering mechanism for cyber-attacks in naval sensors and systems, Sensors 21 (2021) 3195.
[104] N. Pelissero, et al., Naval cyber-physical anomaly propagation analysis based on a quality assessed graph, in: 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), IEEE, 2020, pp. 1–8.
[105] C. Iphar, et al., An expert-based method for the risk assessment of anomalous maritime transportation data, Appl. Ocean Res. 104 (2020), 102337.
[106] S. Jakovlev, et al., Analysis of the Possibility to Detect Fake Vessels in the Automatic Identification System, in: 2020 61st International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), IEEE, 2020, pp. 1–5.
[107] E.P. Marcos, et al., Interference awareness and characterization for GNSS maritime applications, in: 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS), IEEE, 2018, pp. 908–919.
[108] E. Alincourt, et al., Methodology for AIS signature identification through magnitude and temporal characterization. OCEANS 2016-Shanghai, IEEE, 2016, pp. 1–6.
[109] G.L. Babineau, et al., A system-aware cyber security method for shipboard control systems with a method described to evaluate cyber security solutions, in: 2012 IEEE Conference on Technologies for Homeland Security (HST), IEEE, 2012, pp. 99–104.
[110] O. Onishchenko, et al., Ensuring Cyber Resilience of Ship Information Systems, TransNav 16 (2022).
[111] P.M. Laso, et al., ISOLA: an Innovative Approach to Cyber Threat Detection in Cruise shipping, in: Developments and Advances in Defense and Security, Springer, 2022, pp. 71–81.
[112] H. Zhao, B. Silverajan, A Dynamic Visualization Platform for Operational Maritime Cybersecurity, in: International Conference on Cooperative Design, Visualization and Engineering, Springer, 2020, pp. 202–208.
[113] B. Silverajan, P. Vistiaho, Enabling cybersecurity incident reporting and coordinated handling for maritime sector, in: 2019 14th Asia Joint Conference on Information Security (AsiaJCIS), IEEE, 2019, pp. 88–95.
[114] O. Jacq, et al., Detecting and hunting cyberthreats in a maritime environment: specification and experimentation of a maritime cybersecurity operations centre, in: 2018 2nd Cyber Security in Networking Conference (CSNet), IEEE, 2018, pp. 1–8.
[115] O. Jacq, et al., Cyber attacks real time detection: towards a cyber situational awareness for naval systems, in: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), IEEE, 2019, pp. 1–2.
[116] N. Pitropakis, et al., Towards the Creation of a Threat Intelligence Framework for Maritime Infrastructures. Computer Security, Springer, 2019, pp. 53–68.
[117] C. Hemminghaus, et al., SIGMAR: ensuring Integrity and Authenticity of Maritime Systems using Digital Signatures, in: 2021 International Symposium on Networks, Computers and Communications (ISNCC), IEEE, 2021, pp. 1–6.
[118] M.C. Struck, J. Stoppe, A Backwards Compatible Approach to Authenticate Automatic Identification System Messages, in: 2021 IEEE International Conference on Cyber Security and Resilience (CSR), IEEE, 2021, pp. 524–529.
[119] Z. Song, et al., A recursive watermark method for hard real-time industrial control system cyber-resilience enhancement, IEEE Trans. Autom. Sci. Eng. 17 (2020) 1030–1043.
[120] A. Aziz, et al., SecureAIS-securing pairwise vessels communications, in: 2020 IEEE Conference on Communications and Network Security (CNS), IEEE, 2020, pp. 1–9.
[121] A. Goudossis, S.K. Katsikas, Towards a secure automatic identification system (AIS), J. Mar. Sci. Technol. 24 (2019) 410–423.
[122] G. Wimpenny, et al., Public key authentication for AIS and the VHF data exchange system (VDES), in: Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018), 2018, pp. 1841–1851.
[123] B. Xing, et al., Enforcement of opacity security properties for ship information system, Int. J. Naval Architec. Ocean Engin. 8 (2016) 423–433.
[124] Y. Wiseman, Protecting Seaport Communication System by Steganography Based Procedures, Int. J. Secur. Appl. 8 (2014) 25–36. Sandy Bay, Tasmania, Australia.
[125] Y. Wang, et al., A trustable architecture over blockchain to facilitate maritime administration for MASS systems, Reliab. Eng. Syst. Saf. 219 (2022), 108246.
[126] C. Grigoriadis, et al., Integrating and Validating Maritime Transport Security Services: initial results from the CS4EU demonstrator, in: 2021 Thirteenth International Conference on Contemporary Computing (IC3-2021), 2021, pp. 371–377.
[127] G. Bour, et al., On the Certificate Revocation Problem in the Maritime Sector, Springer International Publishing, Cham, 2021, pp. 142–157.
[128] Ø.J. Rødseth, et al., The need for a public key infrastructure for automated and autonomous ships, in: IOP Conference Series: Materials Science and Engineering, IOP Publishing, 2020, 012017.
[129] C. Frøystad, et al., Protecting future maritime communication, in: Proceedings of the 12th International Conference on Availability, Reliability and Security, 2017, pp. 1–10.
[130] W.P. Freire, et al., Towards a Secure and Scalable Maritime Monitoring System Using Blockchain and Low-Cost IoT Technology, Sensors 22 (2022) 4895.
[131] R. Sahay, et al., CyberShip-IoT: a dynamic and adaptive SDN-based security policy enforcement framework for ships, Future Generation Comput. Syst. 100 (2019) 736–750.
[132] T.R.B. Kushal, et al., Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system, IEEE Trans. Smart Grid 10 (2018) 4741–4750.
[133] C.-.G. Yi, Y.-.G. Kim, Security testing for naval ship combat system software, IEEE Access 9 (2021) 66839–66851.
[134] A. Amro, V. Gkioulos, Communication and Cybersecurity Testbed for Autonomous Passenger Ship, in: European Symposium on Research in Computer Security, Springer, 2021, pp. 5–22.
[135] C. Hemminghaus, et al., BRAT: a BRidge Attack Tool for cyber security assessments of maritime systems, TransNav 15 (2021).
[136] J.O. Eichenhofer, et al., An in-depth security assessment of maritime container terminal software systems, IEEE Access 8 (2020) 128050–128067.
[137] B. Croteau, et al., Alternative actuation paths for ship applications in the presence of cyber-attacks. 2019 Resilience Week (RWS), IEEE, 2019, pp. 91–97.
[138] B. Svilicic, et al., Paperless ship navigation: cyber security weaknesses, J. Transport. Secur. 13 (2020) 203–214.
[139] B. Svilicic, et al., Towards a Cyber Secure Shipboard Radar, J. Navig. (2019) 1–12.
[140] B. Svilicic, et al., Shipboard ECDIS cyber security: third-party component threats, Pomorstvo 33 (2019) 176–180.
[141] B. Svilicic, et al., Assessing ship cyber risks: a framework and case study of ECDIS security, WMU J. Maritime Affairs 18 (2019) 509–520.
[142] O.S. Hareide, et al., Enhancing navigator competence by demonstrating maritime cyber security, J. Navigation 71 (2018) 1025–1039.
[143] M. Balduzzi, et al., A security evaluation of AIS automated identification system, in: Proceedings of the 30th annual computer security applications conference, ACM, 2014, pp. 436–445.
[144] S. Khandker, et al., Cybersecurity Attacks on Software Logic and Error Handling Within AIS Implementations: a Systematic Testing of Resilience, IEEE Access 10 (2022) 29493–29505.
[145] D.-.C. Lee, et al., Simulation Testing of Maritime Cyber-Physical Systems: application of Model-View-ViewModel, complex. 2022 (2022).
[146] M. Pavlinović, et al., Cyber Risks in Maritime Industry–Case Study of Croatian Seafarers, in: International Conference on Human Interaction and Emerging Technologies, Springer, 2021, pp. 108–113.
[147] S. Karamperidis, et al., Maritime Cyber Security: a Global Challenge Tackled through Distinct Regional Approaches, J. Mar. Sci. Eng. 9 (2021) 1323.
[148] V. Knight, M. Sadok, Is cyber-security the new lifeboat? An exploration of the employee's perspective of cyber-security within the cruise ship industry, in: 7th International Workshop on Socio-Technical Perspective in IS development (STPIS 2021), CEUR Workshop Proceedings, 2021, pp. 216–231.
[149] C. Senarak, Cybersecurity knowledge and skills for port facility security officers of international seaports: perspectives of IT and security personnel, Asian J. Ship. Logis. 37 (2021) 345–360.
[150] C. Senarak, Port cybersecurity and threat: a structural model for prevention and policy development, Asian J. Ship. Logis. 37 (2021) 20–36.
[151] D. Heering, Ensuring Cybersecurity in Shipping: reference to Estonian Shipowners, TransNav 14 (2020).
[152] J.I. Alcaide, R.G. Llave, Critical infrastructures cybersecurity and the maritime sector, Transport. Res. Procedia 45 (2020) 547–554.
[153] A.R. Lee, H.P. Wogan, All at Sea: the Modern Seascape of Cybersecurity Threats of the Maritime Industry. OCEANS 2018 MTS/IEEE Charleston, IEEE, 2018, pp. 1–8.
[154] J.-.H. Lim, et al., Recent trends and proposed response strategies of international standards related to shipbuilding equipment big data integration platform, Qual. Quant. (2022) 1–22.
[155] L. Drazovich, et al., Advancing the State of Maritime Cybersecurity Guidelines to Improve the Resilience of the Maritime Transportation System, in: 2021 IEEE International Conference on Cyber Security and Resilience (CSR), IEEE, 2021, pp. 503–509.
[156] S.M. Pappalardo, et al., Multi-sector Assessment Framework–a New Approach to Analyse Cybersecurity Challenges and Opportunities, in: International Conference on Multimedia Communications, Services and Security, Springer, 2020, pp. 1–15.
[157] R. Hopcraft, K.M. Martin, Effective maritime cybersecurity regulation–the case for a cyber code, J. Indian Ocean Region 14 (2018) 354–366.
[158] D. Trimble, et al., A framework for cybersecurity assessments of critical port infrastructure, in: 2017 International Conference on Cyber Conflict (CyCon US), IEEE, 2017, pp. 1–7.
[159] K. Bernsmed, et al., Visualizing cyber security risks with bow-tie diagrams. International Workshop on Graphical Models For Security, Springer, 2017, pp. 38–56.
[160] S. Papastergiou, et al., CYSM: an innovative physical/cyber security management system for ports, in: International Conference on Human Aspects of Information Security, Privacy, and Trust, Springer, 2015, pp. 219–230.
[161] S. Papastergiou, N. Polemi, Harmonizing commercial port security practices & procedures in Mediterranean Basin, in: IISA 2014, The 5th International Conference on Information, Intelligence, Systems and Applications, IEEE, 2014, pp. 292–297.

[162] N.A.R. Al Ali, et al., Cyber security in marine transport: opportunities and legal challenges, Pomorstvo 35 (2021) 248–255.
[163] D.L. de Faria, The impact of cybersecurity on the regulatory legal framework for maritime security, JANUS. NET 11 (2020) 163–184.
[164] V. Greiman, Navigating the cyber sea: dangerous atolls ahead, in: Proceedings of the 14th International Conference on Cyber Warfare and Security, Stellenbosch, South Africa, 2019, pp. 87–93.
[165] T. Ramluckan, The Applicability of the Tallinn Manuals to South Africa, in: ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019, Academic Conferences and publishing limited, 2019, p. 348.
[166] O. Daum, Cyber security in the maritime sector, J. Mar. L. & Com. 50 (2019) 1.
[167] R. Hopcraft, Developing Maritime Digital Competencies, IEEE Commun. Stand. Magazine 5 (2021) 12–18.
[168] G. Potamos, et al., Towards a Maritime Cyber Range training environment, in: 2021 IEEE International Conference on Cyber Security and Resilience (CSR), IEEE, 2021, pp. 180–185.
[169] O. Jacq, et al., The Cyber-MAR Project: first Results and Perspectives on the Use of Hybrid Cyber Ranges for Port Cyber Risk Assessment, in: 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021, pp. 409–414.
[170] K. Kuhn, et al., COVID-19 digitization in maritime: understanding cyber risks, WMU J. Maritime Affairs 20 (2021) 193–214.
[171] V. Shapo, M. Levinskyi, Means of Cyber Security Aspects Studying in Maritime Specialists Education. Interactive Mobile Communication, Technologies and Learning, Springer, 2019, pp. 389–400.
[172] A. Androjna, et al., AIS data vulnerability indicated by a spoofing case-study, Appl. Sci. 11 (2021) 5015.
[173] A. Androjna, et al., Assessing cyber challenges of maritime navigation, J. Mar. Sci. Eng. 8 (2020) 776.
[174] M.S.K. Awan, M.A. Al Ghamdi, Understanding the vulnerabilities in digital components of an integrated bridge system (IBS), J. Mar. Sci. Eng 7 (2019) 350.
[175] K. Tam, K. Jones, Forensic readiness within the maritime sector, in: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), IEEE, 2019, pp. 1–4.
[176] E. Erstad, et al., An operational approach to maritime cyber resilience, TransNav (2021) 15.
[177] H. Hutschenreuter, et al., Ontology-based Cybersecurity and Resilience Framework. ICISSP, 2021, pp. 458–466.
[178] V. Engström, R. Lagerström, Two decades of cyberattack simulations: a systematic literature review, Comp. Secur. 116 (2022), 102681.
[179] G. Bour, et al., On the certificate revocation problem in the maritime sector, in: Nordic Conference on Secure IT Systems, Springer, 2020, pp. 142–157.
[180] G. Kavallieratos, et al., SafeSec Tropos: joint security and safety requirements elicitation, Comp. Stand. Interfaces 70 (2020), 103429.
[181] M.S. Karim, Maritime cybersecurity and the IMO legal instruments: sluggish response to an escalating threat? Mar. Policy 143 (2022), 105138.