TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 16
Number 2
June 2022

DOI: 10.12716/1001.16.02.14

Ethical Considerations in Maritime Cybersecurity Research

A. Oruc
Norwegian University of Science and Technology, Gjøvik, Norway

ABSTRACT: Maritime transportation, an essential component of world trade, is performed by contemporary vessels. Despite the improvements that rapid advances in technology have brought to vessels' operational efficiency and capability for safe navigation, the cyber risks associated with modern systems have increased apace. Widespread publicity regarding cyber incidents onboard ships has sparked extensive research on the part of universities, industry, and governmental organisations seeking to understand cyber risks. Consequently, researchers have discovered and disclosed an increasing number of threats and vulnerabilities in this context, providing information that in itself may pose a threat when accessed by the wrong parties. Thus, this paper aims to raise researchers' awareness of ethical concerns and provide guidance for sound decision-making in areas where the research process must be handled carefully to avoid harm. To this end, this paper presents a literature review that explores the ethical issues involved in maritime cybersecurity research and provides specific examples to promote further understanding. Six ethical principles and four categories of ethical dilemmas are discussed. Finally, the paper offers recommendations that can guide researchers in dealing with any ethical conflicts that may arise while studying maritime cybersecurity.

1 INTRODUCTION

Transportation is accepted as a critical infrastructure in the view of many countries, including the USA [1], the EU [2] and Norway [3]. One transportation mode involves waterways and relies exclusively on vessels [4]. In fact, cargo vessels execute over 80% of world trade by volume [5]. Besides carrying cargo around the world, vessels serve other purposes, as well. Today, over 620,000 vessels sail for different purposes, not only transporting cargo but supporting a variety of other endeavours, such as training, research, and fishing [6]. Modern vessels are equipped with many information technology (IT) and operational technology (OT) systems for various purposes, such as navigation, propulsion, communication, cargo handling, safety, and security. However, a major drawback of advancing technology is cyber risks. Numerous cyber incidents affecting onboard ships have been disclosed to date [7,8]. Moreover, much research has revealed the cyber vulnerabilities of modern vessels' computerised systems.

Ethics represent societal beliefs; along these lines, ethical behaviour is generally described as accepted and universal norms [9]. Research ethics is the implementation of ethical principles in application of ethical principles to research activities, including the regulation of research, design and implementation of research, respect for society, the use of resources, and outputs [10]. Ethical committees for research activities in the world (e.g. Norwegian National Research Ethics Committees) operate to provide awareness and encourage the implementation of generally accepted ethical principles [11]. Moreover, various associations (e.g. World Medical Association (WMA)) have issued proclamations of ethical principles in specific research fields (e.g. WMA Declaration of Helsinki - Ethical principles for medical research involving human subjects) [12]. Importantly, even though ethical norms may be linked with legislation, legislation is no substitute for morality [13]. Accordingly, researchers should be fully aware of ethical guidelines and the ethical acceptability of their investigative intent before performing a study [14].

Maritime cybersecurity research and its ethical norms differ from other areas of cyber research in several dimensions. While, in general, each researcher is responsible for anticipating the potential drawbacks that may arrise from their research, in the area of maritime cybersecurity, researchers are obligated to consider the implications and potential repercussions of their research from a wider perspective. Maritime transportation is typically an international mode of transportation performed by a multinational crew. The research process may impact negativelty many vessels operating under the flags of different states and crew members from many countries. As a result, international conflicts may arise during or after research. In many fields, researchers should, in general, avoid damaging a component or system over the course of an investigation. In the case of maritime cyber research, this concern has a wider scope. Assessing risks, including such possibilities as asset damage as well as the environmental and safety impacts of a potential marine accident, is the ethical responsibility of a researcher in this field. One difference that sets the maritime context apart from other fields is its unique work culture. A researcher should respect and be familiar with the dominant culture while participating in research, especially onboard a ship. Currently, both the amount of research and the number of researchers working in this field are relatively smaller than is characteristic of many of the longer-established research domains, such as finance, energy, and communication. However, the need for qualified researchers is highly likely to increase sharply in the future because of the growing digitalisation that is taking place in the maritime industry. As part of accommodating this critically necessary increase, researchers should support the training of junior researchers in this field. For all these reasons, the professional responsibilities of researchers studying maritime cybersecurity are greater than in other fields.

Given that maritime cybersecurity is a relatively new research field, any guiding ethical norms have not yet been defined. The field has seen an increase in research trends, additional academic positions becoming available, and research projects focused specifically on maritime cybersecurity. Such growth points to the need for researchers and responsible authorities to discuss ethical issues in order to establish and ultimately follow ethical guidelines. Accordingly, this study addresses ethical principles and potential dilemmas in maritime cybersecurity research and provides specific examples to illustrate the points made herein. Thus, the study findings will assist researchers and responsible authorities in the case of any ethical conflicts regarding maritime cybersecurity studies. The study findings may prove useful for researchers and institutes working in collaboration with industry, as well.

The study is organised as follows. Section two presents a review of the related literature, followed by a discussion of methodology used in the study in section three. In section four, ethical principles and dilemmas in maritime cybersecurity studies are identified. Consequently, section five offers a summary and suggests additional research topics for further investigation.

2 RELATED WORK

The book *Ethics of Cybersecurity* [15] comprises three parts: foundations, problems, and recommendations. The foundation section provides an introduction to cybersecurity and relevant topics, such as threats and defences in terms of software security, network security, and data security. Next, the book presents a discussion of problems associated with the topic. Examples taken from the book include the ethical paradox, freedom of political communication, and ethical and unethical hacking. Finally, recommendations are proposed, such as norms for states engaging in cyberspace and a framework for ethical cyber defence for companies.

In a representative white paper [16], the authors outline ethical discourse and conflicts of cybersecurity in three domains (health, business, and national security), organised into four aspects (moral character, a literature review summary, identification of ethical issues, and domain-specific value characterisation). The differences between domains are also explained. Lastly, the paper provides a bibliometric analysis of publications, including the number of papers published per year and per domain, the geographic origin of various papers, funding, and citation patterns.

The authors of [17] describe ethical norms of scientific research. Ethical principles in the study are divided into three categories, which comprise ethical scientific inquiry, ethical conduct and behaviours of researchers, and ethical treatment of research participants. Such categories are matched with ethical principles of duty to society, beneficence, conflict of interest, informed consent, integrity, non-discrimination, nonexploitation, privacy and confidentiality, professional competence, and professional discipline. The book also addresses emerging ethics topics, such as big data, open data, and open science.

The authors of the book *Ethics and Policies for Cyber Operations* [18] focus on the ethical issues surrounding accused state-sponsored cyberattacks. One chapter in particular presents a summary of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) workshop on *Ethics and Policies for Cyber Warfare* in 2014. A crucial finding of this workshop is that regulations for cyber warfare are inadequate and require specific definition because of ethical concerns. The author of [19] similarly mentions the lack of recognition of ethical issues in cyberwarfare and goes on to clarify the relationship between cyberwar and traditional war. Specifically, governments may initiate either cyberwar or traditional war as a response to any kind of attack.

Another book [9] focuses on two aspects of IT ethics. First, the author explains in layman's terms the importance of ethics in IT. Second, the book aims to help managers in the IT sector create a work environment where ethical rules are followed. The book provides a comprehensive view of ethics in IT through its discussion of different aspects, such as software development, intellectual property, ethics for IT workers and IT users, and the ethics of IT organisations. Along similar lines, [13] describes the ethical responsibilities of cybersecurity professionals and organisations.

The authors of [20] investigate ethics in cybersecurity research through an examination of two cases. This paper also discusses ethical dilemmas and recommends developing a code of conduct for cybersecurity research to overcome these dilemmas. Such a code may protect researchers against legal claims and assist them in acting in the face of ethical barriers in their research field.

Research papers are available to discuss ethical matters in different fields, such as business, social science, medicine, and veterinary science. However, studies addressing ethical issues have not been applied to the maritime in any detail. Several resolutions issued by the International Maritime Organization (IMO) describe ethical issues affecting organisational concerns [21,22]. Additionally, the author of [23] suggests that maritime training should include a component where ethical decision-making is taught. Ultimately, while various papers and books focused on ethics in cybersecurity research are currently available, none of these addresses specifically to maritime cybersecurity research. Thus, this paper seeks to fill this gap in the field.

3 MATERIALS AND METHODS

A literature review forms the foundation of this study. Scientific databases, including Springer Link, Science Direct, and Taylor & Francis Online, were searched. Google Scholar, ResearchGate, Academia.edu, and Web of Science were also searched to seek out additional relevant publications. Books, journal articles, and conference papers in English were considered. Only publications concerning research ethics – in particular, research ethics in cybersecurity – were considered. The discovered ethical principles and dilemmas were classified and investigated in detail. Citavi software [24] was used to extract data from the articles and manage the acquired knowledge. In the next step, irrelevant principles and dilemmas in relation to maritime cybersecurity research were eliminated. Finally, the paper was enriched with cases and examples of maritime cybersecurity.

Additionally, the IMODOCS and IMO-Vega Database were used to discover cybersecurity-related activities in the IMO. The IMO-Vega Database, developed jointly by the IMO and DNV, maintains historical data and provides up-to-date IMO requirements [25]. The IMODOCS is the official web platform offered by the IMO to make IMO documents available for IMO member governments, intergovernmental agencies, and organisations in consultative status with the IMO [26].

The IMODOCS has several membership access levels with different limitations. The author was accepted via the *IMO Internship Programme*, which is designed for master students and Ph.D. candidates [27]. This status allowed the author to access the IMODOCS with the membership authority of the *IMO Secretariat (Maritime Knowledge Centre)*. The membership level gave the author the same access authority as delegates of member states in the IMO, meaning that the author could access more IMO documents and records not available to the general public.

4 RESEARCH ETHICS IN MARITIME CYBERSECURITY

Over the past decade, interest in maritime cybersecurity has been increasing every year, as can be seen in the results found by searching services such as the Google Trends website, which offers statistics on the current search trends on Google [28]. Google Trends presents values in the form of a graph based on user-specified search terms and time frames. These values range from a minimum of 0 (which can also indicate insufficient data for analysis) to a maximum of 100. Figure 1 displays the results of a worldwide search for the keyword *maritime cybersecurity* for the period spanning 1 January 2012 to 31 December 2021. Google Trends provides data in monthly increments; these monthly values were averaged to yield cumulative by year, as shown in figure 1, to facilitate a better understanding of the trend.

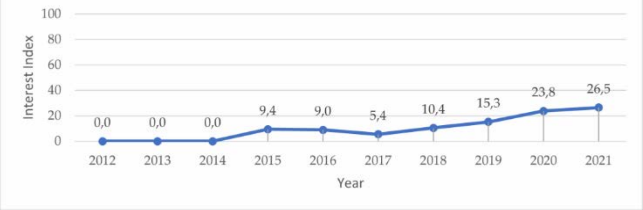

Figure 1. Google Trends search for the keyword *maritime cybersecurity*

Data for the term *maritime cybersecurity* first became detectable by Google Trends in 2015, and the levels remained relatively consistent for the next few years. However, starting in 2017, the Google Trends results demonstrate an increasing trend for this term every year. Seeking to understand the reasons behind this trend led to a search for the keyword *cyber* on the IMODOCS platform. The term appears in the first cybersecurity-related document issued by the IMO, which was published on 10 July 2014 and concerned a proposal by Canada to develop guidelines on maritime cybersecurity [29]. Not long after, two more cybersecurity-related documents were published in September 2014 [30,31]. Conceivably, three mentions in IMO documents issued in 2014 might have led to the first increase that Google Trends indicates for 2015.

The steadily increasing trend in searches related to this topic since 2017 may also be connected to documents published that year. On 16 June 2017, the IMO issued *Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems*, which imposed various requirements on maritime companies after 1 January 2021 [32]. This resolution might represent the originating factor that motivated individuals' interest in maritime cybersecurity.

Since 2014, the IMO has kept up-to-date on maritime cyber security. As of 6 February 2022, a total of 45 IMO documents that reference cybersecurity issues could be located through the IMO-Vega Database and IMODOCS. The latest of these was published on 2 December 2021 and concerned a proposal by the Republic of Korea to develop relevant provisions for cybersecurity-related training for seafarers for possible inclusion in the Standards of Training Certification and Watchkeeping (STCW) Convention [33].

In recent years, numerous research projects have focused on cybersecurity in the maritime sector, such as Maritime Cyber Resilience (MarCy) [34], Cyber Security in Merchant Shipping – Service Evolution (CySiMS-SE) [35], Cyber-MAR [36], Cyber Resilience for the Shipping Industry (CyberShip) [37], and Cyber Security of Maritime ICT-Based Systems [38]. Maritime projects that include cybersecurity-related tasks are also available, such as SFI AutoShip [39]. Moreover, in addition to the aforementioned projects, universities have established several academic positions in the interest of conducting research focused on maritime cybersecurity [40–45]. Furthermore, maritime cybersecurity centres have been established by universities as well as governmental or non-governmental organisations [46–48]. Centres in service have conducted research activities to identify preventive measures to preclude cyber incidents in the maritime domain, given seminars, and provided training. Moreover, they take a role in monitoring, detecting, and responding to cyber incidents.

Careful consideration of current IMO activities, research advances and tendencies leads to the logical conclusion that research on maritime cybersecurity will actively continue in the future. Accordingly, prudence dictates the necessity to identify ethical principles and discuss ethical dilemmas.

4.1 *Ethical Principles in Maritime Cybersecurity Research*

Maritime cybersecurity research should meet six ethical principles, which include integrity, professional responsibility, accountability, confidentiality, legality, and openness.

4.1.1 *Integrity*

Integrity refers to researchers' truthfulness and honesty [17]. Three elements that a researcher must strictly avoid are fabrication, falsification, and plagiarism [49]. Fabrication refers to the invention of data or a case [50]. Falsification denotes the intentional distortion of data or results [50]. Plagiarism means the copying of ideas, data, or statements without citation [50].

Only individuals who contribute to the manuscript significantly should be named as authors. Ghost or gift authorships are not acceptable in academia. Ghost authorship means that although individuals make a significant contribution in terms of writing or revising a manuscript or in performing research, they are not listed in the manuscript as authors [51]. Gift authorship is also known as honorary authorship and guest authorship. Gift authorship, which is the opposite of ghost authorship, refers to individuals who are named as authors in the manuscript even though they have not made a significant contribution to the manuscript [51].

The researcher must be honest regarding the data, results, and research objective in interpreting the research results. Findings should be explained fully. Bias and personal opinions must be avoided. The data, research process, and results must be examined multiple times to avoid potential errors in the study. Unpublished research results should not be used or presented without the permission of the other authors. Moreover, any publication that has been used in the research should be clearly cited. The quality of the paper should be considered, in particular. Potential conflicts of interest should be clearly declared [49]. Some authors publish their own articles in journals where they take in charge as the editor. This approach should be avoided. While a paper of another author is presented, this issue should be declared clearly in required slides or stated verbally at the beginning or end of the presentation.

4.1.2 *Professional Responsibility*

Given that maritime cybersecurity is a relatively new research field, fewer researchers are available in the field compared to other cybersecurity-oriented fields of study. The improvement of a research field depends on highly qualified researchers. Maritime cybersecurity is a challenging area featuring unusual devices comprising terrestrial or aerial systems, including the Electronic Chart Display and Information System (ECDIS), Inmarsat-C, e-Loran, Automatic Identification System (AIS), and the Global Maritime Distress Safety System (GMDSS). Researchers in the field should educate, train, recommend, support, and encourage other scholars who are at an early point in their careers to extend and improve the research field. Understanding of ethical issues as well as technical knowledge should be transferred. The researchers should also strive to attract young people from different backgrounds, such as electrical engineering, computer science, and maritime.

Researchers should be selected according to their qualifications, including sea service, shore experience, enthusiasm, research productivity, and knowledge. Other personal characteristics should be disregarded, such as gender, sexual orientation, nationality, political view, and religious belief. The lead researchers should be fair and treat all members of the research group equally.

Researchers should endeavour to familiarise themselves with national and international maritime culture, including hierarchical structure, especially if the research is performed onboard with seafarers. A strict hierarchy might be implemented onboard due to national maritime culture (e.g. Turkish maritime culture). Inappropriate behaviour on the part of the researcher would not be taken lightly.

4.1.3 *Legality*

Each researcher is responsible for obeying local rules and regulations, like all other individuals. Some cybersecurity research could lead to a conflict with legislation. Several types of components onboard ships use wireless communication protocols, such as satellite or very high frequency (VHF) communications. One such component is the Global Positioning System (GPS), which is a type of Global Navigation Satellite System (GNSS) technology developed by the USA to facilitate detecting the position of the vessel employing this tool. A GPS receiver can be adversely affected by jamming attacks [52]. Thus, it is a matter of concern that several types of GPS jamming devices are currently available on the market [53]. However, the use of such devices may be prohibited by legal authorities of states like in the USA [54]. Therefore, researchers must be fully familiar with legal issues before beginning a study. If required and if possible, the researcher must contact legal authorities to obtain the requisite permissions.

All requirements that are stipulated in signed agreements must be followed. For example, many industries employ non-disclosure agreements (NDAs) [55], such as the NDA established between the Norwegian Maritime Cyber Resilience Centre (NORMA Cyber) and the MarCy project to enable information sharing and support common situational awareness. Furthermore, maritime cybersecurity-related research projects may involve industry partners. Examples of industrial partners in such projects include the Naval Group in Cyber-MAR, NAVTOR in CySiMS-SE, and Kongsberg Defence and Aerospace in MarCy. Various cyber vulnerabilities in the products developed by partners might be detected during a study. In such a case, any action taken must follow the signed agreements.

A researcher should neither exploit nor allow any other person to exploit a detected vulnerability. In the case of such a situation, legal authorities, as well as maritime authorities, if required, should be informed immediately of all considerations involving the potential harms of the exploitation.

4.1.4 *Accountability*

Researchers are also accountable to take all possible protective actions before starting a study. The study methodology should minimise all potential risks, including asset (e.g. cargo, vessel, and component) or environmental damage and safety hazards. During a study, the researcher should care for the components onboard a ship and avoid damage. Any damage to a component, such as ECDIS, gyro compass, and AIS, can lead to a loss of the vessel's seaworthiness. Thus, the sailing of the vessel could be forbidden by maritime authorities (e.g. port state or flag state authorities) until the damaged components are fixed. Mooring the vessel in port may result in mooring costs or penalties due to charter party agreements. Moreover, services needed to repair a damaged component may be costly in terms of both time and money. In such a case, the researcher might be accused of negligence. Additionally, the researcher or sponsoring institution may be held accountable to pay costs or repair any damage to marine systems [15].

A research project may affect more than a single vessel, possibly even many vessels in a specific zone. For instance, as research concerning GNSS may affect the GNSS systems of many vessels in the zone, the research project could precipitate a potential marine accident in the zone. Thus, before starting a study, researchers must lay the appropriate groundwork due to their accountability to consider many different aspects involved, such as vessel traffic, sea and weather conditions, voyages, charter party agreements, and asset value, before starting a study.

Each researcher is totally accountable for his own contribution to the research. Accordingly, the researcher should be able to explain and defend the study, including the selected method, findings, tools and data.

4.1.5 *Confidentiality*

Maritime companies might avoid disclosing the onboard cyber incidents their vessels have encountered because of commercial concerns. Besides commercial vessels, warships can also experience cyber incidents; however, nations' naval forces avoid publicising such incidents because of national security concerns. Accordingly, incidents should not be shared without the permission of the related parties.

Scholars may conduct studies in collaboration with elements of the maritime industry. For instance, vessels in service can be used to conduct pen tests [56,57]. The results of such a pen test should not be available to anyone, including the crew on board, other than nominated staff in maritime companies and should not be published in any environment (e.g. academic article in a journal, or popular science paper in a magazine) without the permission of the maritime company.

A study has the potential to discover cyber vulnerabilities in any onboard systems, which may endanger the safe navigation of the vessel [52,58]. After a paper's publication, malicious actors may exploit any vulnerabilities exposed by attacking vessels in service. A potential marine accident because of such a cyberattack may result in the loss of lives, injuries, and damage to the environment, cargo, and the vessel itself. Seaworthiness or the cargoworthiness of the ship may be lost. Therefore, before disclosing vulnerabilities in equipment, ethical researchers should inform the manufacturers while also allowing them time to eliminate the vulnerabilities in their products.

The personal data of crew, passengers, and office staff associated with research should be strictly protected. Various research centres maintain research data, such as the Norsk Senter for Forskningsdata (NSD – Norwegian Centre for Research Data) in

Norway, which offers secure storage of research data. The centre archives a wide range of research data, allowing research-based access while protecting the privacy of individuals and organisations.

4.1.6 *Openness*

Researchers should always consider the well-being of the maritime industry with all stakeholders, such as IMO, seafarers, cadets, shipping companies, class societies, flag states, manufacturers, and any other governmental and non-governmental organisations. Moreover, researchers should maximise the research benefit, which includes what information should be disseminated, as well as how this should be done, as a significant topic. Research results should be shared with stakeholders using language that is suited to the appropriate technical level for the intended audience. General information aimed at the entire maritime community might entail publishing popular science papers in maritime magazines to explain cyber vulnerabilities. In contrast, academic articles, along with seminars and workshops, could target professionals working on maritime cybersecurity.

Openness improves credibility and trust. A research report should clearly describe the implemented method as well as all tools used and the research findings. Moreover, the data set and developed tools used in the study should be shared through platforms (e.g. GitHub) if no restrictions are required (e.g. the necessity to prevent the selling of data sets or weaponisation of the tool). In this way, other researchers will be able to replicate the research using the same data and method to confirm the accuracy of the obtained results. Researchers should always be open to critique.

Detected vulnerabilities in the components and actual cyber incidents in the maritime industry should be disclosed by remembering malicious actors who can exploit such vulnerabilities, as mentioned in section 4.1.5. This approach to information sharing can improve cyber resilience in the maritime industry.

4.2 *Ethical Dilemmas in Maritime Cybersecurity Research*

The field of maritime cybersecurity, like many research fields, includes various ethical dilemmas. Thus, an ethical committee in an organisation or, alternatively, an external ethical committee could be beneficial in coping with such ethical dilemmas [59]. Hence, this section explains ethical dilemmas relating to maritime cybersecurity studies.

4.2.1 *Research on State-Sponsored Cyberattacks*

Cybersecurity for states is another facet of national security. Cyberattacks may be performed for different military purposes, such as cyber espionage, surveillance, and disruption of the target systems [60]. Furthermore, civilians, including the attacking states in states' own citizens, may be affected by state-sponsored cyberattacks [15].

Civilian vessels are operated for a variety of purposes, including training, commercial, research, rescue, and so on. However, because of national defence research, many civilian vessels are affected by state-sponsored cyberattacks [8]. In 2019, the U.S.-based non-profit Center for Advanced Defence Studies (C4ADS) released a report entitled *Above Us Only Stars*. According to this report, 1,311 civilian vessels were affected over a two-year period by Russian GNSS spoofing attacks [8]. Given that several navigation components on the bridge, such as AIS and ECDIS, require GNSS connection, the GNSS system is of critical importance in terms of the safe navigation of the vessels. Such cyberattacks may cause loss of seafarer lives, environmental pollution, and asset damage as a result of a marine accident. Another reason states may engage in cyberattacks is to gather information from other countries. For example, the Danish Maritime Authority was subjected to cyberattack for two years [61]. According to the Danish Defence Intelligence Service (Forsvarets Efterretningstjeneste), these attacks were carried out by Chinese officials who were attempting to capture sensitive information about Danish maritime companies and the country's merchant navy [62].

As this discussion has shown, civilian vessels and the private marine industry are potential targets of state-sponsored attacks. Thus, the question arises as to whether research supporting the development of novel cyberattack methods for the benefit of the researcher's own country is even ethical.

4.2.2 *Developing Services and Tools*

Services and tools that are developed for security assessment may be accessible to anyone. However, such services and tools can help malicious actors, in addition to system administrators, detect insecure systems. Thus, developing and launching these services leads to ethical dilemmas. [63]

Internet services that allow for continuous monitoring, such as Shodan.io and Censys.io, are available to support system administrators. These services scan the internet constantly and provide results on their websites. Users of these services can obtain the results they need through a full-text search. A Very Small Aperture Terminal (VSAT) onboard a ship offers two-way satellite communications for internet, data and telephony [64]. As previously mentioned, Shodan.io is available to support researchers and system administrators alike. Additionally, because Shodan.io also provides VSAT-related results, a malicious actor may exploit the results that this service publishes [65].

Vulnerability detection tools are useful for security analysts who can take precautions against cyber risks. However, the tools offer equally effective weapons for attackers, even though they do not constitute harmful software on their own. Tools can be developed for a study and distributed on public platforms (e.g. GitHub) as part of a scientific publication. However, it bears repeating that malicious actors can exploit such tools as weapons.

Various tools have been developed for security assessment of marine systems in particular, such as the BRidge Attack Tool (BRAT) [66]. Because of the possibility of attacks that target systems on the bridge, the authors of the BRAT might prefer not to share the details of this tool in the open literature. In another study, the researchers only partially shared information in GitHub about tools used in AIS vulnerability research because of the risk of weaponisation [58,67].

4.2.3 *Sharing Details of Actual Cyber Incidents*

Information sharing about actual cyber incidents can be fruitful to enhance awareness, decrease vulnerabilities, manage risk, and improve cyber resilience [68]. Stakeholders in the maritime industry may take a position against potential cyberattacks or contribute to mitigation. Contrariwise, malicious actors can also realise the vulnerability and possibly attack other potential victims in the industry by exploiting the disclosed vulnerability. Cyber incident reports consist of various information types, such as threats, vulnerabilities, measures, recommendations, and analysis [69]. Besides their intended uses, such reports may also be used as training material by malicious actors intending an attack.

In one case, a malicious actor took full control of the navigation system of a container vessel for 10 hours [7]. No technical details from this incident are available in the open literature. Nevertheless, because many vessels might have similar vulnerabilities, the same type of attack is also a danger to their safe navigation. Disclosing the details would have compelled other companies in the maritime industry to take precautions against the vulnerability. Contrariwise, disclosing the attack details bears the risk of attracting other potential attackers, who could use such details to exploit the exposed vulnerabilities. These reasons underlie the difficulty in deciding what information about an actual cyber incident to share in a research paper [69].

4.2.4 *Other Dilemmas*

As previously mentioned, a research project might be performed with the collaboration of product developers. A stakeholder in such a project may request a vulnerability analysis for a specific marine component that they neither use nor produce. It is highly possible that such a product could be related to a competitor. Because a researcher cannot ensure how the stakeholder will use a possible vulnerability that is detected, accepting or rejecting such a request by the researcher represents a conflict. [70]

During a research investigation, the researchers may detect a critical vulnerability in a component. Even when researchers allow the vendors time to correct the problem, the manufacturers might not fix the issue or disclose it for various reasons, such as fear of loss of reputation or a negative financial impact on the company. Such a potential vulnerability may open the possibility for marine incidents to occur, leading to harm to seafarers, vessels, or the environment. In the event of an agreement between the parties (e.g. an NDA), the agreement might hamper the ability to inform the maritime community about potential vulnerabilities.

One of the foremost conflicts in cybersecurity is situated between personal privacy and security [71,72]. For example, VSAT technology has made the internet more accessible to seafarers today. Cybersecurity research on a live ship network may make seafarers' sensitive data more accessible to researchers. Specifically, such research may involve logging, monitoring, and analysing seafarers' activities in the network, including their internet activity.

5 CONCLUSION

Maritime cybersecurity has attracted increasing attention, accelerating in recent years, as illustrated by the growth indicated by Google Trends on this topic. This growing focus underlines the potential benefit of investigating ethical issues associated with maritime cybersecurity research. This study examined maritime cybersecurity in terms of ethical issues, including ethical principles and ethical dilemmas. Key ethical principles identified were integrity, professional responsibility, legality, accountability, openness, and confidentiality. Ethical dilemmas were also described, such as ethical dilemmas in developing tools and services, conducting research in support of state-sponsored cyberattacks, and sharing details in a research paper concerning cyber incidents that have occurred.

Sharing the details of an actual cyber incident is a necessary component of preventing potential further cyberattacks. However, the details should be restricted to a specific group, with carefully selected group members, to prevent such information from being exploited by malicious actors. Such a group may also share developed tools for cybersecurity assessment onboard vessels for use in further studies. In practice, developers currently do not share such tools in the open literature in order to preclude malicious usage. For this reason, researchers should request any needed tool from developers directly if required. However, developers cannot ensure the proper use of such developed tools.

During the research process, the differences between the membership levels *public users* and *IMO Secretariat (Maritime Knowledge Centre)* were evident in the IMODOCS. Circulars, meeting documents, and programmes are open to all users. However, circular letters, meeting audio-recordings, notes verbales, and treaties are additional areas accessible via the account setting of *IMO Secretariat (Maritime Knowledge Centre)*. In particular, meeting audio-recordings are useful, especially in that they provide the ability to hear the discussions of member states in the IMO meetings. Future studies may find such discussions regarding maritime cyber security invaluable in their investigations.

Ethics can be considered as the public conscience. Thus, when a conflict arises without an obvious solution, working out the appropriate resolution may involve choosing to take the "right" action over what might appear at first glance to be the expedient answer.

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to IMO, in particular, the Maritime Knowledge Centre and External Relations Office, for their support and hospitality during my attendance in the IMO Internship Programme.
This paper has received funding from the Research Council of Norway through the Maritime Cyber Resilience (MarCy, projectNumber 295077) project. The content reflects only the authors' views, and neither the Research Council of Norway nor the project partners are responsible for any use that may be made of the information it contains.

REFERENCES

1. CISA. Transportation systems sector. Available online: https://www.cisa.gov/transportation-systems-sector (accessed on 29 March 2021).
2. Mattioli, R.; Levy-Bencheton, C. *Methodologies for the identification of Critical Information Infrastructure assets and services;* ENISA, 2015, ISBN 978-92-9204-106-9.
3. Nystuen, K.O.; Hagen, J.M. Critical Information Infrastructure protection in Norway. In *Informatik,* Frankfurt, Germany, 29 September 2003 - 02 October 2003, 2003.
4. Zhao, X.; Yang, Z.; Yang, Z.; Feng, Y. Study on the choice of transportation mode for regional logistics. In *6th Conference of the Eastern-Asia-Society-for-Transportation-Studies*, Bangkok, Thailand, 2005; pp 16–31.
5. UNCTAD. *Review of maritime transport 2021*, New York, USA, 2021. Available online: https://unctad.org/webflyer/review-maritime-transport-2021 (accessed on 20 November 2021).
6. VesselFinder. Vessel database. Available online: https://www.vesselfinder.com/vessels (accessed on 29 April 2021).
7. Blake, T. Hackers took 'full control' of container ship's navigation systems for 10 hours - IHS Fairplay | RNTF. Available online: https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-ihs-fairplay/ (accessed on 25 March 2020).
8. C4ADS. Above us only stars: Exposing GPS spoofing in Russia and Syria. Available online: https://www.c4reports.org/aboveusonlystars (accessed on 14 April 2021).
9. Reynolds, G.W. *Ethics in information technology*, 5th ed.; Cengage Learning, 2015, ISBN 978-1-285-19715-9.
10. University of Stirling. Understanding ethics. Available online: https://www.stir.ac.uk/research/research-ethics-and-integrity/understanding-ethics/ (accessed on 28 December 2021).
11. Forskningsetikk. About us. Available online: https://www.forskningsetikk.no/en/about-us/ (accessed on 27 December 2021).
12. WMA. *WMA Declaration of Helsinki - Ethical principles for medical research involving human subjects*, 2013. Available online: https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/ (accessed on 4 January 2022).
13. Hamburg, I.; Grosch, K.R. Ethical aspects in cyber security. *Archives of Business Research* **2017**, *5*, doi:10.14738/abr.510.3818.
14. Aguinis, H.; Henle, C.A. Ethics in research. In *Handbook of research methods in industrial and organizational psychology;* Rogelberg, S.G., Ed.; Blackwell, 2002.
15. *The ethics of cybersecurity;* Christen, M.; Gordijn, B.; Loi, M., Eds.; Springer International Publishing: Cham, 2020, ISBN 978-3-030-29052-8.
16. Yaghmaei, E.; van de Poel, I.; Christen, M.; Gordijn, B.; Kleine, N.; Loi, M.; Morgan, G.; Weber, K. *Canvas White Paper 1 - Cybersecurity and ethics*, 2017.
17. Weinbaum, C.; Landree, E.; Blumenthal, M.S.; Piquado, T.; Gutierrez, C.I. *Ethics in scientific research*: *An examination of ethical principles and emerging topics;* RAND: Santa Monica CA, 2019, ISBN 9781977402691.
18. Taddeo, M.; Glorioso, L. *Ethics and policies for cyber operations;* Springer International Publishing: Cham, 2017, ISBN 978-3-319-45299-9.
19. Dipert, R.R. The ethics of cyberwarfare. *Journal of Military Ethics* **2010**, *9*, 384–410, doi:10.1080/15027570.2010.536404.
20. Macnish, K.; van der Ham, J. Ethics in cybersecurity research and practice. *Technology in Society* **2020**, *63*, doi:10.1016/j.techsoc.2020.101382.
21. IMO. *Resolution MSC.349(92) Code for recognized organizations (RO Code) Part 2 - Recognition and authorization requirements for organizations;* IMO: London, UK, 2013.
22. IMO. *Resolution A.1136(31) Ethical considerations and guidelines for conduct of IMO Council election campaigns;* IMO: London, UK, 2019.
23. Moore, T.R. Ethics and the maritime profession: An argument for teaching in maritime training and strategies for making ethical decisions. In *International Asscociation of Maritime Universities Proceedings of Inaugular General Assembly,* Istanbul, Turkey, 26 June 2000 - 29 June 2000, 2000.
24. Citavi. Reference management and knowledge organization. Available online: https://citavi.com/en (accessed on 4 February 2022).
25. IMO. The IMO-Vega Database. Available online: https://www.imo.org/en/publications/Pages/IMO-Vega.aspx (accessed on 5 February 2022).
26. IMO. About IMODOCS. Available online: https://docs.imo.org/Default.aspx (accessed on 4 February 2022).
27. IMO. IMO Internship Programme. Available online: https://www.imo.org/en/About/Careers/Pages/Internship-default.aspx (accessed on 8 February 2022).
28. Choi, H.; Varian, H. Predicting the present with Google Trends. *Economic Record* **2012**, *88*, 2–9, doi:10.1111/j.1475-4932.2012.00809.x.
29. IMO. *FAL 39/7 Ensuring security in and facilitating international trade. Measuring toward enhancing maritime cybersecurity.;* IMO: London, UK, 2018.
30. IMO. *MSC 94/4/1 Measures to enhance maritime security. Measures toward enhancing maritime cyber security;* IMO: London, UK, 2014.
31. IMO. *FAL 39/WP.8 Proposal for new output on the development of guidelines on the facilitation aspects of protecting the maritime transport network from cyber threats;* IMO: London, UK, 2014.
32. IMO. *Resolution MSC.428(98) Maritime cyber risk management in Safety Management Systems;* IMO: London, UK, 2017.
33. IMO. *HTW 8/15/1 Any other business. Necessity of developing relevant provisions concerning cybersecurity-related training for seafarers.;* IMO: London, UK, 2021.
34. CRISTIN. Maritime Cyber Resilience. Available online: https://app.cristin.no/projects/show.jsf?id=2057306 (accessed on 29 April 2021).

35. CySiMS-SE. Cyber Security in Merchant Shipping Service Evolution (CySiMS-SE). Available online: http://cysims.no/ (accessed on 26 January 2022).
36. Cyber-MAR. About. Available online: https://cyber-mar.eu/about/ (accessed on 29 April 2021).
37. DTU. Project CyberShip. Available online: https://www.cybership.man.dtu.dk/english/overview. (accessed on 4 May 2021).
38. University of Rijeka. Cyber security of maritime ICT-based systems **2019**.
39. NTNU. Work package 2: Digital infrastructure. Available online: https://www.ntnu.edu/sfi-autoship/digital-infrastructure (accessed on 29 April 2021).
40. DTU. Postdoc in cyber resilience for the shipping industry. Available online: https://computeroxy.com/postdoc-in-cyber-resilience-for-the-shipping-industry,i4678.html (accessed on 30 April 2021).
41. EURAXESS. ERA chair holder, professor of cybersecurity in maritime domain. Available online: https://euraxess.ec.europa.eu/jobs/582237 (accessed on 1 May 2021).
42. iTrust. Cyber risk management study in shipboard OT systems. Available online: https://itrust.sutd.edu.sg/maritime/ (accessed on 4 May 2021).
43. Jobbnorge. PhD position in maritime cyber security. Available online: https://www.jobbnorge.no/en/available-jobs/job/167349/phd-position-in-maritime-cyber-security (accessed on 4 May 2021).
44. THE. PhD candidate in maritime cyber resilient operations. Available online: https://www.timeshighereducation.com/unijobs/listing/182718/phd-candidate-in-maritime-cyber-resilient-operations/ (accessed on 4 May 2021).
45. TalTech. *Maritime cyber security*, 2018.
46. Danish Maritime Cybersecurity Unit. Cyber and information strategy for the maritime sector 2019 - 2022. Available online: https://dma.dk/Media/637709330853499994/Cyber%20and%20Information%20Security%20Strategy%20for%20the%20Maritime%20Sector.pdf (accessed on 1 May 2021).
47. MPA. New 24/7 Maritime Cybersecurity Operations Centre to boost cyber defence readiness. Available online: https://www.mpa.gov.sg/web/portal/home/media-centre/news-releases/detail/8a5114cf-8214-4b46-8999-2c6c42433b1e (accessed on 4 May 2021).
48. NORMA Cyber. About NORMA. Available online: https://www.normacyber.no/en/about (accessed on 25 December 2021).
49. King, N. Research ethics in qualitative research. In *Doing qualitative research in psychology: A practical guide,* 2nd ed.; Sullivan, C., Forrester, M.A., Eds.; SAGE, 2019; pp 35–59.
50. Fanelli, D. How many scientists fabricate and falsify research? A systematic review and meta-analysis of survey data. *PLoS One* **2009**, *4*, e5738, doi:10.1371/journal.pone.0005738.
51. Kennedy, M.S.; Barnsteiner, J.; Daly, J. Honorary and ghost authorship in nursing publications. *J. Nurs. Scholarsh.* **2014**, *46*, 416–422, doi:10.1111/jnu.12093.
52. Grant, A.; Williams, P.; Ward, N.; Basker, S. GPS jamming and the impact on maritime navigation. *J. Navigation* **2009**, *62*, 173–187, doi:10.1017/S0373463308005213.
53. The Signal Jammer. GPS jammer. Available online: https://www.thesignaljammer.com/products/GPS-Jammer.html (accessed on 2 May 2021).
54. National Coordination Office for Space-Based Positioning, Navigation, and Timing. Information about GPS jamming. Available online: https://www.gps.gov/spectrum/jamming/ (accessed on 2 May 2021).
55. Blackshaw, I.S. Confidentiality and Non-Disclosure Agreements. In *Sports Marketing Agreements: Legal, Fiscal and Practical Aspects*; Blackshaw, I.S., Ed.; T. M. C. Asser Press: The Hague, The Netherlands, 2012; pp 67–72, ISBN 978-90-6704-792-0.
56. Svilicic, B.; Rudan, I.; Jugović, A.; Zec, D. A study on cyber security threats in a shipboard Integrated Navigational System. *Journal of Marine Science and Engineering* **2019**, *7*, 364, doi:10.3390/jmse7100364.
57. Svilicic, B.; Kristić, M.; Žuškin, S.; Brčić, D. Paperless ship navigation: cyber security weaknesses. *Journal of Transportation Security* **2020**, *13*, 203–214, doi:10.1007/s12198-020-00222-2.
58. Balduzzi, M.; Pasta, A.; Wilhoit, K. A security evaluation of AIS automated identification system. In *Proceedings of the 30th Annual Computer Security Applications Conference on - ACSAC '14*, New Orleans, Louisiana, 08–12 Dec. 2014; Payne, C.N., Butler, K., Sherr, M., Hahn, A., Eds.; ACM Press: New York, USA, 2014; pp 436–445.
59. Jaquet-Chiffelle, D.-O.; Loi, M. Ethical and unethical hacking. In *The ethics of cybersecurity*; Christen, M., Gordijn, B., Loi, M., Eds.; Springer International Publishing: Cham, 2020; pp 179–204, ISBN 978-3-030-29052-8.
60. Cavelty, M.D. Breaking the cyber-security dilemma: aligning security needs and removing vulnerabilities. *Sci. Eng. Ethics* **2014**, *20*, 701–715, doi:10.1007/s11948-014-9551-y.
61. Cyber Keel. Maritime cyber-risks. Available online: https://sfmx.org/wp-content/uploads/2017/03/Maritime-Cyber-Crime-10-2014.pdf (accessed on 25 July 2022).
62. The Local. State-sponsored hackers spied on Denmark. Available online: https://thelocal.dk/20140922/denmark-was-hacked-by-state-sponsored-spies (accessed on 15 April 2021).
63. Herrmann, D.; Pridöhl, H. Basic concepts and models of cybersecurity. In *The ethics of cybersecurity*; Christen, M., Gordijn, B., Loi, M., Eds.; Springer International Publishing: Cham, 2020; pp 11–44, ISBN 978-3-030-29052-8.
64. Marlink. What is maritime VSAT? Available online: https://marlink.com/what-is-maritime-vsat/ (accessed on 11 May 2021).
65. Chambers, S. Ship's satellite communication system hacked with ease. Available online: https://splash247.com/ships-satellite-communication-system-hacked-ease/ (accessed on 11 May 2021).
66. Hemminghaus, C.; Bauer, J.; Padilla, E. BRAT: A BRidge Attack Tool for cyber security assessments of maritime systems. *TransNav: The International Journal on Marine Navigation and Safety of Sea Transportation* **2021**, *15*, 35–44, doi:10.12716/1001.15.01.02.
67. GitHub. Toolkit for research purposes in AIS. Available online: https://github.com/trendmicro/ais (accessed on 6 January 2022).
68. Luiijf, E.; Klaver, M. On the sharing of cyber security information. In *Critical Infrastructure Protection IX*; Rice, M., Shenoi, S., Eds.; Springer International Publishing: Cham, 2015, ISBN 978-3-319-26566-7.

69. Albakri, A.; Boiten, E.; Lemos, R. de. Risks of sharing cyber incident information. In *ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security,* Hamburg Germany, 27–30 Aug. 2018; ACM: New York, USA, 2018; pp 1–10, ISBN 9781450364485.

70. Kirichenko, A.; Christen, M.; Grunow, F.; Herrmann, D. Best practices and recommendations for cybersecurity service providers. In *The ethics of cybersecurity*; Christen, M., Gordijn, B., Loi, M., Eds.; Springer International Publishing: Cham, 2020; pp 299–316, ISBN 978-3-030-29052-8.

71. van de Poel, I. Core values and value conflicts in cybersecurity: Beyond privacy versus security. In *The ethics of cybersecurity*; Christen, M., Gordijn, B., Loi, M., Eds.; Springer International Publishing: Cham, 2020; pp 45–71, ISBN 978-3-030-29052-8.

72. Christen, M.; Gordijn, B.; Loi, M. Introduction. In *The ethics of cybersecurity*; Christen, M., Gordijn, B., Loi, M., Eds.; Springer International Publishing: Cham, 2020; pp 1–8, ISBN 978-3-030-29052-8.