JOURNAL OF MARITIME RESEARCH

Vol XXI. No. I (2024) pp 97–100

ISSN: 1697-4840, **www.jmr.unican.es**

A review of Ethical Considerations within Autonomous Maritime Cybersecurity Research

Björn John Praestegaard Larsen[1,*]

ARTICLE INFO

Article history:
Received 7 Aug 2023;
in revised from 24 Aug 2023;
accepted 13 Oct 2023.

Keywords:
Ethics, Research, Maritime, Cyber Security.

ABSTRACT

The paper covers some of the ethical considerations and principles that researchers need to consider while conducting research within the field of autonomous maritime cyber security. It starts with a brief introduction to the research area and the cyber security risks associated with this. Then moves on to address the ethical considerations that researchers must consider. Basic research principles such as honesty, transparency, objectivity, independence, accountability, and fairness are emphasised. Additionally, the paper briefly explores an important socio-technical consideration, industry-sponsored research, and the potential conflicts of interest that arise when conducting such research. The conclusion highlights the importance of conducting ethical research with a high level of transparency.

1. Introduction.

Autonomous configurations are defined by the ability to make decisions without interacting with humans (Brodsky, 2016; Collingwood, 2017; Suchman & Weber, 2016). In their present form autonomous maritime vessels, land-based vehicles, and industry-related units, which are considered autonomous, still depend on humans as the operators (Ramos et al., 2018). It is difficult to predict with certainty what the future will demand from humans in terms of operational routines (Komianos, 2018; Mallam et al., 2020). From the maritime angle cyber security risks onboard vessels are commonly discussed by dividing digital environments into two categories: operational technology (OT) and information technology (IT) (Lagouvardou, 2018; Larsen & Lund, 2021). Within the maritime sector three major categories of research have been identified. (1) Detailed documentation of policies and important know-how relating to maritime cybersecurity, (2) cybersecurity related to ports, and (3) vulnerabilities of OT (Awan & Al Ghamdi, 2019).

2. Background.

Contemporary research is subject to a public image of being conducted by individuals which shows heightened levels of ethics, often including being reliable, accurate, transparent, and always working in the best interest of society (Oliver, 2010). Still, even though researchers can assume that they will be accountable for their publications and that this involves being as unbiased as possible (Bos, 2020), there has been an increasing amount of Questionable Research Practices (QRPs) over the last 20 years (Bruton et al., 2020; Gopalakrishna et al., 2022; Isbell et al., 2022). For the context of this document, it is important to understand that maritime cybersecurity research is still very much in its infancy and there are a small number of researchers active within the industry (Oruc, 2022).

3. Method.

To be able to collect relevant data the following approach has been embraced for this unstructured literature review. The scope of the research has been defined using terminology such as ethical research, maritime research and autonomous maritime research. Furthermore a list of what is to be considered important keywords within this field has been compiled and used to search academic databases, search engines, and other

[1]Jönköping University, P.O. Box 1026, 551 11 Jönköping, Sweden.
[*]Corresponding author: Björn John Praestegaard Larsen. E-mail Address: bjorn.larsen@ju.se.

sources for gathering literature, including university libraries and search engines such as Google Scholar. Selection has been made from relevance, publication date and quality.

4. Considerations.

Ethics is used as an individual compass for determining what is acceptable, it is based on personal moral conviction, society enforced rules and regulations together with both social and cultural heritage (Hamburg & Grosch, 2017). Not surprisingly there are increased demands within the academical profession when it comes to experience and the knowledge within different methodologies for conducting research in a manner which can be considered ethical (Navalta et al., 2019).

There is a consensus that we should develop and enhance technology and social behaviour in conjunction with each other to advance both aspects at the same time (Taxén, 2020). In this regard, cybersecurity can be defined as a function of the interactions between various technological and social factors that make up complex, adaptive socio-technical systems (Kowalski, 1994). As a result, researchers within any area of cyber security will likely at one point or another come across information during their research which could be considered private (Macnish & Van der Ham, 2020). In all such cases it is important for the researcher to abide by the laws and regulations to determine which information can be processed and how (Loi & Christen, 2020). This should be applied both in the context of following international as well as local legislations, something that could possibly interfere with experiments and data collection (Burstein, 2008). It all comes down to the key ingredient of consent when conducting research which involves individuals, something which has been emphasised since the Nurmberg trials and the Helsinki declaration (Association et al., 2001; Code, 1949; Weindling, 2001). This is or should be a human right by default and its fundamental value was established already by Brandeis and Warren (1890) with their conclusion of every individuals right to be let alone.

5. Principles.

There are ethical principles presented within the research community which serve as guidelines for researchers to conduct their work with integrity and accountability (Kretser et al., 2019). These principals emphasise importance of honesty, transparency, objectivity, independence, accountability, and fairness in research practices (ALLEA, 2017; Drenth, 2012; Vetenskapsrådet, 2017). It should be acknowledged that the field of research ethics within cybersecurity has been subject to numerous attempts to standardise ethical principles (Bailey et al., 2012; Loi & Christen, 2020; Morgan et al., 2020; van de Poel, 2020; Weber & Kleine, 2020).

Industry sponsored research raises several ethical considerations that researchers should be aware of (Stahl et al., 2019). Several studies states that industry sponsored research might be designed to generate results that support the sponsor's interests (Djulbegovic et al., 2000; Fabbri et al., 2018). Researchers need to be aware that potential conflicts of interest can arise when conducting industry sponsored research, not surprisingly this might be conflicts of a financial kind (Fabbri et al., 2018; Smith, 2006). In fact, there is a growing opinion that such financial conflicts of interest might jeopardise the reputation of the whole research field (Resnik, 2000).

Conclusions.

Ethical research is of utmost importance for researchers across all fields. It can be concluded that in many cases it is the researcher who must choose to conduct research in an ethical manner (Fujii, 2012). This should include disclosing any financial or personal interests that could affect the objectivity of their research carried out. Furthermore, researchers must respect privacy laws such as General Data Protection Regulation 2016/679 (GDPR) (European Parliament and the European Council (EP/EC), 2016) and of course any other international and/or local regulations which might be applicable. In all cases within the field of autonomous maritime cybersecurity research, principals of how to conduct ethical research should be taken into consideration and that the results of any industry sponsored research are reported both accurately and fully transparently. In conclusion, researchers which are conducting industry sponsored research shall remain vigilant to potential ethical concerns and make sure that the research carried out is conducted with the highest standards of ethical conduct regarding design, execution, and that all reporting is made in a manner which is independent, transparent, and scientifically valid.

As a researcher it should be the ambition to abide to the laws and regulations which apply for any specific field and for research in general, but also to follow existing ethical guidelines such as those described within The European Code of Conduct for Research Integrity (ALLEA, 2017), always striving to conduct ethically sound research with as high level of transparency as is possible and by doing so helping in maintaining the public's trust in the research enterprise.

References.

ALLEA. (2017). The European Code of Conduct for Research Integrity. All European Academies.

Association, W. M., et al. (2001). World Medical Association Declaration of Helsinki. Ethical principles for medical research involving human subjects. Bulletin of the World Health Organization, 79(4), 373.

Awan, M. S. K., & Al Ghamdi, M. A. (2019). Understanding the vulnerabilities in digital components of an integrated bridge system (IBS). Journal of Marine Science and Engineering, 7(10), 350.

Bailey, M., Dittrich, D., Kenneally, E., & Maughan, D. (2012). The menlo report. IEEE Security & Privacy, 10(2), 71–75.

Bos, J. (2020). Research Ethics for Students in the Social Sciences. Springer Nature. doi: 10.1007/978-3-030-48415-6.

Brandeis, L., & Warren, S. (1890). The right to privacy. Harvard law review, 4(5), 193–220.

Brodsky, J. S. (2016). Autonomous vehicle regulation: How an uncertain legal landscape may hit the brakes on self-driving cars. Berkeley Technology Law Journal, 31(2), 851–878.

Bruton, S. V., Brown, M., & Sacco, D. F. (2020). Ethical consistency and experience: An attempt to influence researcher attitudes toward questionable research practices through read.ing prompts. Journal of Empirical Research on Human Research Ethics, 15(3), 216– 226. doi: 10.1177/1556264619894435.

Burstein, A. J. (2008). Conducting cybersecurity research legally and ethically. LEET, 8, 1–8.

Code, N. (1949). The nuremberg code. Trials of war criminals before the Nuremberg military tribunals under control council law, 10(1949), 181–2.

Collingwood, L. (2017). Privacy implications and liability issues of autonomous vehicles. Information & Communications Technology Law, 26(1), 32–45.

Djulbegovic, B., Lacevic, M., Cantor, A., Fields, K. K., Bennett, C. L., Adams, J. R., Lyman, G. H. (2000). The uncertainty principle and industry-sponsored research. The Lancet, 356(9230), 635–638.

Drenth, P. J. (2012). A European code of conduct for research integrity. In T. Mayer & N. Steneck (Eds.), Promoting Research Integrity in a Global Evironment (p. 161). World Scientific Publishing Co. Pte. Ltd.

European Parliament and the European Council (EP/EC). (2016). Regulation (EU) General Data Protection Regulation 2016/679 (GDPR). Official Journal of the European Union.

Fabbri, A., Lai, A., Grundy, Q., & Bero, L. A. (2018). The influence of industry sponsorship on the research agenda: A scoping review. American journal of public health, 108(11), e9–e16.

Fujii, L. A. (2012, October). Research Ethics 101: Dilemmas and Responsibilities. PS: Political Science & Politics, 45(4), 717–723. doi: 10.1017/S1049096512000819.

Gopalakrishna, G., Ter Riet, G., Vink, G., Stoop, I., Wicherts, J. M., & Bouter, L. M. (2022). Prevalence of questionable research practices, research misconduct and their potential explanatory factors: A survey among academic researchers in The Netherlands. PloS one, 17(2), e0263023.

Hamburg, I., & Grosch, K. R. (2017). Ethical aspects in cyber security. Archives of Business Research, 5(10), 199–206. doi: 10.14738/abr.510.3818.

Isbell, D. R., Brown, D., Chen, M., Derrick, D. J., Ghanem, R., Arvizu, M. N. G., ... Plonsky, L. (2022). Misconduct and questionable research practices: The ethics of quantitative data handling and reporting in applied linguistics. The Modern Language Journal, 106(1), 172–195.

Komianos, A. (2018). The autonomous shipping era. operational, regulatory, and quality challenges. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 12(2).

Kowalski, S. (1994). IT insecurity: A multi-disciplinary inquiry. Stocholm: Kungliga Tekniska Högskolan.

Kretser, A., Murphy, D., Bertuzzi, S., Abraham, T., Allison, D. B., Boor, K. J., ... others (2019). Scientific integrity principles and best practices: Recommendations from a scientific integrity consortium. Science and Engineering Ethics, 25, 327–355.

Lagouvardou, S. (2018). Maritime Cyber Security: Concepts, problems and models. Kongens Lyngby, Copenhagen.

Larsen, M. H., & Lund, M. S. (2021). Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review. IEEE Access : Practical innovations, Open solutions, 9, 144895–144905. doi: 10.1109/ACCESS.2021.3122433.

Loi, M., & Christen, M. (2020). Ethical frameworks for cybersecurity. In M. Christen, B. Gordijn, & M. Loi (Eds.), The Ethics of Cybersecurity (Vol. 21). Springer International Publishing.

Macnish, K., & Van der Ham, J. (2020). Ethics in cybersecurity research and practice. Technology in society, 63, 101382.

Mallam, S. C., Nazir, S., & Sharma, A. (2020). The human element in future Maritime Operations–perceived impact of autonomous shipping. Ergonomics, 63(3), 334–345.

Morgan, G., Gordijn, B., & Loi, M. (Eds.). (2020). The Ethics of Cybersecurity (Vol. 21). Springer Open.

Navalta, J. W., Stone, W. J., & Lyons, T. S. (2019). Ethical issues relating to scientific discovery in exercise science. International journal of exercise science, 12(1), 1.

Oliver, P. (2010). The student's guide to research ethics. McGraw-Hill Education (UK).

Oruc, A. (2022). Ethical Considerations in Maritime Cybersecurity Research. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 16(2), 309–318. doi: 10.12716/1001.16.02.14.

Ramos, M. A., Utne, IB., & Mosleh, A. (2018). On factors affecting autonomous ships operators performance in a Shore Control Center. Proceedings of the 14th Probabilistic Safety Assessment and Management, Los Angeles, CA, USA, 16–21.

Resnik, D. B. (2000). Financial interests and research bias. Perspectives on Science, 8(3), 255–285.

Smith, R. (2006). Conflicts of interest: How money clouds objectivity. Journal of the Royal Society of Medicine, 99(6), 292–297.

Stahl, B. C., Chatfield, K., Ten Holter, C., & Brem, A. (2019). Ethics in corporate research and development: Can responsible research and innovation approaches aid sustainability? Journal of Cleaner Production, 239, 118044.

Suchman, L., & Weber, J. (2016). Human-machine autonomies. Autonomous weapons systems: Law, ethics, policy, 75–102.

Taxén, L. (2020, April). Reviving the Individual in Sociotechnical Systems Thinking. Complex

Systems Informatics and Modeling Quarterly (2), 39–48. doi: 10.7250/csimq.2020-22.03 van de Poel, I. (2020). Core values and value conflicts in cybersecurity: Beyond privacy versus security. In M. Christen, B. Gordijn, & M. Loi (Eds.), The Ethics of Cybersecurity (Vol. 21, pp. 45–71). Springer International Publishing.

Vetenskapsrådet. (2017). Good research practice. Stockholm: Swedish research council.

Weber, K., & Kleine, N. (2020). Cybersecurity in health care. In M. Christen, B. Gordijn, & M. Loi (Eds.), The Ethics of Cybersecurity (Vol. 21, pp. 139–156). Springer International Publishing.

Weindling, P. (2001). The origins of informed consent: The international scientific commission on medical war crimes, and the Nuremberg Code. Bulletin of the History of Medicine, 37–71.