frontiers | Frontiers in Computer Science

TYPE Editorial
PUBLISHED 13 February 2024
DOI 10.3389/fcomp.2024.1378160

OPEN ACCESS

EDITED AND REVIEWED BY
Nicola Zannone,
Eindhoven University of Technology, Netherlands

*CORRESPONDENCE
Adam Turner
adam.turner07@gmail.com

RECEIVED 29 January 2024
ACCEPTED 30 January 2024
PUBLISHED 13 February 2024

CITATION
Turner A, McCombie SJ and Uhlmann AJ (2024) Editorial: The impacts of cyber threat in the maritime ecosystem.
Front. Comput. Sci. 6:1378160.
doi: 10.3389/fcomp.2024.1378160

Editorial: The impacts of cyber threat in the maritime ecosystem

Adam Turner[1]*, Stephen James McCombie[2] and Allon J. Uhlmann[3]

[1]Macquarie University, Sydney, NSW, Australia, [2]NHL Stenden University of Applied Sciences, Leeuwarden, Netherlands, [3]Thorbecke Academy, NHL Stenden University of Applied Sciences, Leeuwarden, Netherlands

KEYWORDS

cyber security, maritime security, intelligence, cyber risk assessment, cyber threat intelligence (CTI)

Editorial on the Research Topic
The impacts of cyber threat in the maritime ecosystem

This Research Topic will present a spotlight on the exposure the maritime industry has to cyber adversaries, and on how the impacts of computer security vulnerabilities have a broader effect on economies and criminal networks. The criticality and fragility of our supply chains have been demonstrated during the COVID-19 Pandemic. This is particularly evident within the Global Maritime Transportation System (GMTS). The GMTS is a system of systems and includes not just vessels but also waterways, ports, and land-side connections, moving people and goods to and from the water. The role of GMTS in the global economy is significant with over 80% of the world's cargo transported by ship (Bronk and deWitte, 2020) and representing 70% of global trade by value (Loomis et al., 2021). At the same time, fleets are aging, and their technology is aging with them and thus they are more vulnerable to cyber-attacks. 38% of oil tankers and 59% of general cargo ships are more than 20 years old (Tam and Jones, 2018). Supply chains themselves are increasingly vulnerable to cyber-attacks. This is particularly stark in recent years, "...European sources estimated a 400% growth in supply chain cyberattacks in 2021 compared to 2020" (Kessler and Shepherd, 2022). GMTS is clearly a key part of global supply chains and will be increasingly targeted by cyber threat actors. Since 2018, state sponsored threat actors from China (amongst others) have specifically targeted the maritime industry (Mandiant, 2018).

In a 2019 report "Shen attack: cyber risk in Asia Pacific ports" – produced by the University of Cambridge Center for Risk Studies, researchers described a hypothetical cyber-attack across the Asia Pacific against 15 ports using malware that jumped from ships to ports. They projected the loss could go as high as USD$110 Billion with the vast majority of that amount not being covered by any insurance (Daffron and Ruffle, 2019). Such a cyber-attack on this scale has not as yet been seen in the maritime sector, but we have seen numerous ports and ships impacted by attacks using ransomware, destructive malware, and the even hacking of Operational Technology (OT). These attacks have been initiated by both criminal groups and nation-state hackers. The well-known case of Maersk which lost over USD$200 million in 2017 in the NotPetya malware attack is a significant example (Matthews, 2017).

In a non-cyber case in March 2020, the MV Evergiven blocked the Suez Canal and caused major disruption to the GMTS. While the incident was caused by human error rather than a cyber-attack it demonstrates the fragility of the GMTS costing some USD$9

Billion per day (Lee and Wong, 2021). Such an incident could easily be deliberately caused by a cyber-attack. The threat actor could achieve this by compromising the navigation or propulsion systems of a ship or in a number of other ways. The aim of such an attack might be a part of a great power conflict (i.e., USA/China), a regional conflict (i.e., Israel/Iran), or by cybercriminals demanding ransom or shorting the stock market.

The aforementioned themes are evident in the body of research collected for this Research Topic. In this article "*Quantifying the econometric loss of a cyber-physical attack on a seaport,*" Tam et al. present the modeling and quantification of how a cyber-attack, with physical consequences, can affect local and global trade. This case study shows the initial economic impacts may start locally but will often lead to global effects if response mechanisms prove insufficient. As a result the researchers produced the five-part CyPEM (Cyber Physical Econometric Model) that has the capability to translate a cyber-attack to an econometric loss. With a system model by Tam et al. for economic impact on modern Cyber-Physical Systems the focus turns to risk management and how digitalization may help improve the efficiency of terminal systems in port processing. However, at the same time the improvement of port processes relies on the development of information and communication technology (ICT) as well as on industrial control systems (ICS) and operation technologies (OT). The cyber security of these systems also needs to be addressed. This is where Pöyhönen and Lehto, proposed a system for cyber security in port and harbor ecosystems in this article "*Comprehensive cyber security for port and harbor ecosystems*." The article emphasizes the importance of a system of systems approach in terms of a comprehensive cyber security management process for port ecosystems. The description and recognition of management steps of every stakeholder are the key elements in this kind of process. Taking motivation from the Finnish maritime Sea4Value program, this article amplifies the importance of port security as identified in the European Union Agency for Cybersecurity (ENISA) report "Port Cybersecurity" (2019) by providing conceptual and architectural insights into security best practices.

Kyranoudi and Polemi, look at a different, but equally as important, market segment when it comes to securing the maritime ecosystem. In this article, "*Securing small and medium ports and their supply chain services*," they focus on the need to secure small and medium sized ports (SMPs) and their supply chain services. SMB operators do not share the large budgets of multinational logistics companies. They argue that SMPs are just as important as larger ports in terms of supply chain service (SCS) management and security. For attackers, they can be an attractive target and form the weakest links for national and European Union (EU) resilience and security. The potential threats and attacks on SMPs and SCSs are analyzed along with basic security concepts. In addition, three SMP attack scenarios are described to illustrate the likelihood of an attack occurring on an SMP, as well as the significance and extent of potential cascading effects. Finally, a risk management methodology for SCSs in SMPs is proposed. This methodology is named CYSMET, and is based on existing SCS risk analysis methods.

Furthermore, Sage, examines a critical maritime navigation component automatic identification systems (AIS). In her article, "*Shining a light on AIS blackouts with maritime OSINT*," Sage examines the vulnerability of AIS communication systems to malicious cyber-attacks. Further focus is applied to the intentional manipulation of AIS data, the real world impacts when AIS communications fail and how open source intelligence (OSINT) can be used to augment the absence of AIS data. The article shows how OSINT is an effective method providing valuable information to target the who, what, where, and why maritime operations may be being obfuscated. A case study of Russian oil exports evading sanctions is provided to demonstrate the ability of the OSINT approach to inform critical compliance programs.

Finally, this Research Topic looks into the future with the emergence of uncrewed Maritime Autonomous Surface Ships (MASS). Fenton and Chapsos in their article, "*Ships without crews: IMO and UK responses to cybersecurity, technology, law and regulation of maritime autonomous surface ships (MASS)*," consider the current technological developments in MASS, the legal and regulatory challenges that they raise, and describes the ways in which an international body (the International Maritime Organization, IMO) and a national agency (UK Maritime and Coastguard Agency, MCA) are engaging with the task of regulating these advancements in the maritime ecosystem. This research draws deep insights through data collected in the field by conducting surveys with industry experts, academics, government and international regulators. The article makes an original contribution by noting and analyzing the approaches of the IMO and the UK government–bodies which are highly influential in shaping global attitudes, preparation, adoption, and responses to emerging technologies like MASS. The research examines how they have engaged with regulating the various legal, technical and cybersecurity challenges MASS raises. It concludes that for the MASS technology to fulfill its potential and gradually see the integration of such vessels in international shipping in a safe, secure and sustainable way, the international community needs to work together, and update by consensus the key legal instruments and policy documents. In this major undertaking, Fenton and Chapsos identify the learning role the UK and IMO can play as the protagonist in developing and implementing best practice.

Author contributions

AT: Writing—original draft. SM: Writing—original draft, Writing—review & editing. AU: Writing—review & editing.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Bronk, C., and deWitte, P. (2020). "Maritime cybersecurity: meeting threats to globalization's great conveyor," in *Proceedings of the Annual Hawaii International Conference on System Sciences*. doi: 10.24251/hicss.2020.240

Kessler, G., and Shepherd, S. (2022). *Maritime Cybersecurity: A Guide for Leaders and Managers, 2nd Edn*. Daytona Beach, FL: Independently Published.

Lee, J. M., and Wong, E. Y. (2021). "Suez Canal blockage: an analysis of legal impact, risks and liabilities to the global supply chain," in *MATEC Web of Conferences*, 339. doi: 10.1051/matecconf/202133901019

Loomis, W., Singh, V. V., Kessler, C. C., and Bellekens, D. (2021). *Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity*. Available online at: https://www.atlanticcouncil.org/in-depth-research-reports/report/raising-the-colors-signaling-for-cooperation-on-maritime-cybersecurity/

Mandiant (2018). *Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S.* Alexandria, VA: Engineering and Maritime Industries.

Matthews, L. (2017). *NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million*. Forbes.

Tam, K., and Jones, K. D. (2018). Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *J. Cyber Policy* 3. doi: 10.1080/23738871.2018.1513053