





Advanced Engineering Days

aed.mersin.edu.tr



Cyber-attack techniques in the maritime industry

Ünal Özdemir*¹, Taha Talip Türkistanlı²

¹Mersin University, Maritime Faculty, Maritime Transportation and Management Engineering, Türkiye
unalozdemir@mersin.edu.tr; tahaturkistanli@mersin.edu.tr

Cite this study: Özdemir, Ü., & Türkistanlı, T. T. (2022). Cyber-attack techniques in the maritime industry. 2nd Advanced Engineering Days, 47-49

Keywords

Maritime
Cyberattacks
MCDM
Fuzzy Logic

Abstract

With the introduction of Industry 4.0, the digital integration of all industries became a significant issue. Concepts such as the internet of things, Blockchain, big data analysis were emphasized as the most popular digital integration instruments. In the maritime industry, globalization led to the most advanced trade networks that included the most advanced and fastest ships, robot-assisted ports and vast computer databases that track cargo. However, although the digital media leads to optimum cost, optimum time, optimum benefits, etc., it also increased the risk of cyberattacks to industry transactions. The rise in cyberattacks is predicted to have the potential to seriously damage the critical infrastructure in the future. Thus, the present study aimed to determine the types of cyberattacks on the maritime industry, and the possible measures that could be adopted to prevent or reduce these attacks with a quantitative approach. Since the data collected in the study were mostly oral data, expert opinions were required, and covariance, overlaps, dependencies between the criteria associated with the research problem, the study was conducted with a fuzzy multi-criteria decision-making (FMCDM) approach.

Introduction

In general, harmful behaviors and actions that could be conducted with viruses, trojans or similar codes, mostly planned and coordinated to attack internet systems are called cyberattacks (Craig et al. 2013; Julisch, 2013; Rid & Buchanan, 2015). The review of recent cyberattacks would demonstrate that their targets were quite diverse, including hacktivism that aim financial or political gain or blackmail, or simply theft (Schaik et al. 2017; Teoh & Mahmood, 2018). Furthermore, while certain cyberattacks have a purpose, other are conducted without any purpose, only to harm the victim or to satisfy the attacker's ego (Liu et al. 2020). The fact that national and international legal sanctions against cyberattacks are not really deterrent is also considered a significant factor in cyberattacks on the maritime industry (Pu and Lam, 2021). Furthermore, cyberattacks to the vessel navigation technologies such as AIS (Automatic Identification System), GNSS (Global Navigation Satellite System) and ECDIS (Electronic Chart Display and Information System) could lead to significant consequences such as rerouting the vessel (Egan et al. 2016). Another type of cyberattack in maritime industry entails rerouting the vessel with false GPS signals and routing the vessel to pirate prone areas. Even when this dangerous attack is noticed, the crew could not intervene to the deck and machinery automation technologies. Cyberattacks could not only target the vessels and navigational equipment, but also other maritime trade units. The attacks in the maritime industry include the alteration of cargo manifests such as renaming illegal shipments such as drugs or weapons as ordinary and non-hazardous freight (Gertzan, 2003; Fitton, 2015; Tucci, 2017; Sivilić et al 2019).

Material and Method

A comprehensive field study and a literature review was conducted to determine the cyberattacks on the maritime industry and to provide solutions. The analyses revealed a large number of written and verbal data. For the numerical analysis of these data, the data should be organized systematically. The authors preferred MCDM methodology to avoid the complex solutions obtained with classical mathematical models since the collected data was large, not systematic, and the verbal expressions and suggestions were significant for the scope of the study. MCDM methods are frequently employed in the literature, and generally provide more effective solutions for these types of problems, lead to a more practical and flexible solutions based on expert opinions (Ting Shih and Gwo-Hsiung, 2004; Özdemir & Güneroğlu, 2015; Wang and Peng, 2015; Özdemir an& Güneroğlu, 2017). Thus, an integrated model approach that included DEMATEL and TOPSIS methods was adopted in the study. In the model, the fuzzy DEMATEL technique was employed to determine the causalities and significance distributions in the study. Then, the fuzzy TOPSIS method, developed by Chen (2000), was employed to calculate the ranking of the solution hypotheses. The DEMATEL and TOPSIS methods were preferred since these are the most adequate methods for the structure of the study, and their implementation is simple and comprehensible.

Results and Discussion

The study findings revealed that the top three ranking cyberattack types were C10 (System Infrastructure Hacks), C4 (System hacks) and C12 (Phishing) on the maritime industry. It could be suggested that the most prevalent type of cyberattack, namely "hacking maritime company web-based systems to demand ransom for allowing access or sharing data with third parties," should be prioritized in future studies conducted by IMO (International Maritime Organization). The past cyberattacks on the maritime industry demonstrated that the main motivation in these attacks was extortion. C4 (System hacks - Changing, disrupting or destroying the content of valuable documents [bill of lading, freight plan, transport contracts, etc.] by hacking the systems of land operations such as the ports and agencies) was the second prevalent type of cyberattack. The study findings on alternative solutions demonstrated that the root solutions for the problem included K3 (Initiation of R&D work to develop mandatory software that would fully protect the land and vessel data systems under the coordination of IMO and inclusion of the employment of this system in international maritime conventions) , K2 (Ensuring the reliability of the IT infrastructure of the International P&I Clubs Group, Bolero and essDOCS systems and the e-title system that provide international electronic bill of lading applications and approved by the International Group of P&I Clubs with approved virus protection systems) and K8 (Network production including software clustering, unauthorized access identification, software whitelists, access and user control mechanisms.) alternatives.

Based on the expert opinions, it was observed that the solution should be organized by IMO. Thus, it was concluded that, IMO should conduct R&D to develop a standard antivirus software compatible with the maritime industry databases and the software should be compulsory and this should be stipulated in international maritime conventions, especially in member countries. It is known that IMO has conducted significant studies on cyberattacks. It could be suggested that the most significant work was the "Guidelines for Cyber Security on board Ships". However, this is only a guide and implementation is voluntary. It is the alternative K2 with the second highest degree of importance that draws attention as a solution to the problem. The second ranked alternative was the K2(Ensuring the reliability of the IT infrastructure of the International P&I Clubs Group, Bolero and essDOCS systems and the e-title system that provide international electronic bill of lading applications and approved by the International Group of P&I Clubs with approved virus protection systems.)

Note

This study has been sent for review and publication to the *International Journal of Transport Economics* by paper author Associate Professor Dr. Ünal ÖZDEMİR. The peer-review process of the study continues.

References

- [1] Chen. C. T. (2000). Extensions of the Topsis for Group Decision-Making Under Fuzzy Environment. *Fuzzy Sets And Systems*, 114 (1):1-9.
- [2] Craigen, D., Diakun-Thibault, N. & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10): 3-21.
- [3] Egan, D., Drumhiller, N., Rose, A. & Tambe, M. (2016). *Maritime Cyber Security University Research: Phase 1* (No. CG-D-07-16). US Coast Guard New, London United States.

- [4] Fitton, O., Prince, D., Germond, B. & Lacy, M. (2015). The future of maritime cyber security. Lancaster University, England.
- [5] Gertjan, V. D. Z (2003). The Legal Underpinning of E-Commerce in Maritime Transport by The Uncitral Draft Instrument on The Carriage of Goods By Sea. The Journal of International Maritime Law, 9(5):461-470.
- [6] Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns”, Computer Networks, 57(1): 2206-2211.
- [7] Liu, Z., Wang, Q. & Tang, Y. (2020). Design of a co-simulation platform with hardware-in-the-loop for cyber-attacks on cyber-physical power systems. IEEE Access,8:95997-96005.doi 10.1109/ACCESS.2020.2995743.
- [8] Özdemir, Ü. & Güneroğlu, A. (2015). Strategic Approach Model for Investigating The Cause of Maritime Accidents”, Scientific Journal on Traffic and Transportation Research, 27:113-123.
- [9] Özdemir, Ü. & Güneroğlu, A. (2017). Quantitative Analysis of the World Sea Piracy by Fuzzy AHP and Fuzzy TOPSIS Methodologies. International Journal of Transport Economics, 44(3):427-448.
- [10] Pu, S. & Lam, J. S. L. (2021). Blockchain adoptions in the maritime industry: A conceptual framework. Maritime Policy & Management, 48(6): 776-794.
- [11] Rid, T. & Buchanan, B. (2015). Attributing Cyber Attacks. Journal of Strategic Studies, 38(1-2): 4-37.
- [12] Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J. & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behavior. Computers in Human Behavior, 75(1): 547-559.
- [13] Svilicic, B., Kamahara, J., Rooks, M. & Yano, Y. (2019). Maritime Cyber Risk Management: An Experimental Ship Assessment. The Journal of Navigation, 72(5): 1108- 1120.
- [14] Teoh, C.S. & Mahmood, A.K. (2018). Cybersecurity Workforce Development for Digital Economy. The Educational Review, 2 (1):136-146.
- [15] Ting, Y. H., Shih, T., L. & Gwo-Hshiang, T. (2004). Fuzzy Mcdm Approach for Planning and Design Tenders Selection In Public Office Buildings. International Journal of Project Management, 22: 573-584.
- [16] Tucci, A.E. (2017). Cyber Risks in the Marine Transportation System. In Cyber-Physical Security. pp. 113-131, Springer International Publishing.
- [17] Wang. X. & Peng. B. (2015). Determining the value of the port transport waters: Based on improved TOPSIS model by multiple regression weighting. Ocean & Coastal Management, 107: 37-45.