Maritime transport sector digitalisation; Is it cyber-secure?

Karamperidis, S; Koligiannis, G

Published in:
Default journal

Publication date:
2020

Stavros Karamperidis
Plymouth Business School
University of Plymouth
United Kingdom
Tel: +44 1752 585589

Email: stavros.karamperidis@plymouth.ac.uk

Georgios Koligiannis
Hellenic Navy
Greece
Tel:+306940103646
Email:gkoligiannis1@gmail.com

Maritime transport sector digitalisation; Is it cyber-secure?

Extended Abstract

Objective

The last twenty years, the maritime transport sector, invested in cutting edge technology to enhance productivity, develop efficient maritime supply chains and facilitate the interactions between several stakeholders. The aforementioned investments in technology assisted the maritime transport sector to decrease its operational costs. To this aim, digital platforms, automation and several technologies including blockchain, and internet of things (IoT) are used by vessels and port authorities. However, as the sector becomes more digitalised the attack surface increases and the potential cyber-actors apply numerous tools to achieve their aims. Several entities were subjected to cyber-attacks recently (e.g. COSCO, etc.), which highlights the need of all the stakeholders to develop and implement proper strategies for an evolving cyber-resilient maritime transport ecosystem. A big challenge is that the operators and the ship-owners will finally understand the threats from a cyber-perspective. The purpose of the research is to present the current cyber-threat landscape in the maritime transport sector and provide solutions to the problem.

Data/Methodology

A mixed-method exploratory study was applied to exploit the benefits provided by both qualitative and quantitative methods. The combination of qualitative and quantitative methods support the triangulation of the findings and a complete understanding of the research problem. Hence, a more holistic picture of the research issue has been provided than either approach alone. In order to tackle the research objectives and due to the novelty of the research problem, primary data were gathered from scholars and practitioners from several sectors, which had suffered in the past notable cyber-attacks. Those findings were supported by a Structured Literature Review (SLR) which was focused in maritime cyber-security. The authors aimed to present the trend in research to maritime cyber-security, to summarise the results of the existing literature, and to identify any research gap. The SLR uses five steps (i.e., question formulation, locating the study, study selection and evaluation, analysis and synthesis, reporting and using the results) as was defined by Denyer and Tranfield (2009). Three online databases (i.e., "Emerald Insight", "Science Direct" and "Taylor and Francis online") were used as search engines in order to retrieve relevant papers that contained the terms "cyber-security", or "cyber-threat", or "cyber-attacks" and "maritime sector". Overall, 462 articles were obtained, and after applying further exclusion criteria, only seven were chosen for further screening, all of them published in different journals. To achieve deep understanding, the SLR was supported by in-depth interviews. To draw useful conclusions from the research, snowball sampling was selected as a strategy for the expert's identification. Overall, twenty interviews were conducted with cyber-security experts from various relevant sectors (i.e. maritime, finance, academia and military). Responses were collected and analysed by using thematic analysis, which helped the authors to highlight differences and similarities of the collected data and generate insights that have not been anticipated.

Results/Findings

According to experts, malicious software is the most prevalent cyber-threat for the maritime transport sector. Academic cyber-expert (1) mentioned: "*Recent incidents have shown that ransomware is very prevalent and so they have been very high-profile cases*". According to participants, cyber-incidents will increase in future, due to the digitalisation of the sector and the low level of cyber-security culture, which was clearly mentioned by several maritime participants: "*The attack surface is getting bigger and bigger. In conclusion, the threat is real, and the risk is high*" *(Maritime cyber-security expert, 1*). Maritime expert 4 mentioned: "*I believe that at the moment the maritime industry has not been identified by the hackers as a target, but very soon they will realise the effects and how easy is to penetrate a vessel, and the whole game will change*". It has also been found that the three most probable impacts in case of a cyber-incident are: **financial losses**, **business disruptions** and **reputation damage**. Maritime cyber-expert 2 stated: "*For now, financial gain is the primary and by far the most significant impact of a cyber-incident*" while a cyber-expert in the defence industry (1)

mentioned: "*The most damaging impact could be the loss of the customers' confidence, which will further cause financial losses and damage to the brand image*". According to the interviewees, the most critical barriers that deter a maritime entity from investing in cyber-security are the **cost of the investment**, **the low level of awareness in the C-level (Chief level)**, **the absence of the mandatory regulation**, and **the scale of the problem in the specific sector**. Notably, maritime cyber-security expert (6) voiced the following view: "*When an entity invests in IT security, you never have visible directly ROI, and usually, as far as I know, investments in IT security come after a significant incident or because the promulgated laws and directives make you invest on it*".

Implications for Research/Policy

If the sector does not address cyber-threats effectively, then digitalisation will prove to be catastrophic. The challenges for the maritime transport sector are significant as it depends on operation technology systems, proprietary devices, and legacy systems that have never been under-research until recently and were designed without taking into account the presence of cyber-threats. As the industry becomes more informed about cyber-enemies, the countermeasures applied will be more customised and more effective. The majority of the interviewees agreed that a holistic approach is needed to face cyber-threats. However, it should not be ignored that the threat-actors will use several tools to achieve their aims depending on the assets of the industry. Each vessel and each port depend on numerous assets designed by different vendors and different specifications that remain unclear to which degree are cyber-secure. Thus, as was highlighted by the experts, a useful tool to identify an entity's vulnerabilities is penetrations testing, which presents potential threats and the level of an entity's cyber-risk... Findings show to the leading entities in the sector that in order to build a cyber-resilient ecosystem they should strive to increase cyber-awareness through **training** and by **implementing information technology countermeasures** such as segmentation of a company's IT networks, implementing back up procedures and security policies based on behaviour analytics. The limitations of the study include the number of respondents that contributed to gathering primary data, as most entities hesitate to reveal information related to cyber-security policies or cyber-incidents. To better understand the implications of a cyber-attack, further work could focus on assessing cyber-risk for a specific port or a specific shipping company which would be helpful for the entity under investigation.

Keywords: *Maritime transport sector, Digitalisation, Cyber-security, Cyber-threats.*