MARITIME STRATEGIC EVALUATION FOR ISRAEL 2021/22

Chief Editor: **Prof. Shaul Chorev**

Editor: **Dr. Ziv Rubinovitz**

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

HMS
Maritime Policy & Strategy Research Cente
המרכז לחקר מדיניות ואסטרטגיה ימית

Estimate of the Cost of Protecting the Sea Ports in Israel Against Cyber Threats[1]

Itai Sela

Introduction

The global economy is dependent on the civil maritime industry to a large extent, not to say completely. The implications of disruption of the supply chain due to cyber attack are not limited to a small number of raw materials-dependent manufacturing sectors; they affect a vast array of consumer products which are dependent on the maritime supply chain.

The weaponization of the cyber space and the increasing involvement of state and non-state players in cyber attacks against critical infrastructures, including the use of private entities and advanced technologies in order to achieve strategic value, make the maritime arena extremely vulnerable. The cyber threat highlights the attacker's advantage and exposes the defender's vulnerabilities. Over the past decade, the civil maritime industry (vessels, passenger ships, shipyards, ports, terminals, and energy infrastructures) has become highly dependent on computer and control systems which are based on operational technology. These systems are mostly based on obsolete operating systems, do not have security updates and patches, have limited (if any) monitoring capabilities, and most of them have no cybersecurity. These technology gaps, the weaknesses caused by the man-machine interface, the reliance on the human factor as a solution for coping with the cyber threat and the reliance on non-binding recommendations, all together make it difficult to analyze the implications and losses actually caused by maritime cyber attacks.

This article analyzes the cyber threat [the act of inserting malware into information technology (hereafter IT) or operational technology (hereafter OT) systems, with the intention of achieving military, intelligence or business objectives] with emphasis on OT systems within the civil maritime industry. It assesses the cost of the threat and the required solution for protecting all of Israel's ports, while recommending a conceptual shift in the cybersecurity of the civil maritime industry.

The main findings in this article indicate that the direct and indirect cost of the cyber threat from a single attack on the four ports in Israel is estimated at an average of

[1] This article is part of my thesis written under the guidance of Prof. Shaul Chorev, Head of the Maritime Strategy & Policy Research Center, The Social Science School International Relations Division, and Dr. Doron Nissani, Business Management School.

approximately $1.7 billion. At the same time, the cost of the solution for that threat according to the proposed 'Inside-Out' cyber defense approach, is estimated at an average of approximately $3.5 million per year, which is less than one quarter of one percent of the cost of the cyber threat itself. Decision-makers called upon to discuss the issue of coping with the cyber threat to the operational systems hesitate to decide as to the investment in cybersecurity for operational systems in their organization due to the complexity, cost and information gaps. However, the intensification of the scope and nature of the cyber attacks on maritime assets in general and on sea ports in particular indicates that the trend is gaining momentum, and that it is becoming more likely that the operational systems of the Israeli sea ports will be attacked in the near future. Therefore, this article reflects the nature of the threat, the defensive concepts and the accounting calculation between the cost of the threat and the cost of the solution, in order to enable decision-makers in Israel (managements and regulators) to assess, from a new perspective, the defensive concept and its cost, against the cost of the threat and the damage which may be incurred as a result of one cyber attack against the sea ports in Israel.

The cyber threat to the civil maritime industry

Over the past decade, industries in general and the maritime industry in particular have become increasingly dependent on OT computer systems serving as a man-machine interface and helping in the management of critical operations. In the civil maritime industry and its components (the shipping sector, ports and terminals sector, shipyards, and energy infrastructures), the operational technology plays significant roles in running critical functions. This technology is based on obsolete, unmonitored operating systems which are not interconnected, and they are dependent on updates and maintenance which is sent from information systems, and which usually do not have cybersecurity. The growing demands made to the maritime industry to increase efficiency and improve the quality of the service it delivers to its customers is totally dependent on the quality of the communication, the logistics, the OT systems and the IT systems, all of which expose the sea ports and the various maritime platforms to cyber attacks, which are on a continual upwards trajectory.[2]

Rid & McBurney (2012) define cyber weapons as malware used to achieve military or intelligence goals as part of a cyber attack. Its appearance has made the maritime industry in general, and the OT systems in particular, more exposed and more

[2] Ido Ben-Moshe and Itai Sela, Maritime Policy & Strategy Research Center, University of Haifa (2020), The cyber threat to the ports front.

vulnerable. In this article, the use of the term 'cyber threat' describes the act of inserting malware into computing systems (OT and IT), with emphasis on the OT systems.

Studies indicate on the one hand that the response to the cyber threat in the maritime arena has been low, that the number of reported attacks does not reflect the actual number of attacks (Jensen, 2015), that the potential inherent to the maritime cyber threat is about to become the most severe business threat in future (Schauer et al, 2017), and the maritime industry is not prepared to cope with these risks in an environment based on modern OT systems (Silgado, 2018).[3] On the other hand, due to understanding of the threat and its potential implications on the world economy, non-binding recommendations have been issued for cyber security in the sea ports and in maritime platforms which are reliant on the human factor. They believe humans are able to successfully cope with the cyber threat and that this is their responsibility. This has been said despite the understanding that human error is the main cause of maritime accidents (Luo & Shin, 2019, Arslan et al., 2016), particularly in an environment rife with technological changes (Pomeroy & Earthy, 2017). This sharpens the gap between the prevailing concept within the industry that still considers the human factor to be the main problem, and the fact that it also singles him out as being responsible for a solution.

In Israel, the government decided in 2011 on "advancing national cyberspace capabilities", and set up the National Cyber Bureau within the Prime Minister's Office.[4] In 2015, the Bureau was renamed National Cyber Directorate,[5] and finally in 2017 it was merged with the National Cybersecurity Authority to form the National Cyber Directorate.[6] In 2015, the government defined the term Cybersecurity as the entirety of the measures intended to prevent, mitigate, investigate and cope with cyber threats and cyber events and to reduce their impact and the damage they cause, prior to their occurrence, while they are occurring and after them. it determined "that protecting the normal, safe functioning of cyberspace is the State's

---

3 Silgado, D.M. (2018). *Cyber-attacks: A digital threat reality affecting the maritime industry*. World Maritime University.

4 Prime Minister's Office, Israel (2011). Government decision 3611, Advancement of the National Capability in Cyberspace [Hebrew]

5 Prime Minister's Office, Israel (2015). Government decision 2443, Advancement of National Regulation and Government Cybersecurity Leadership [Hebrew].

6 Prime Minister's Office, Israel (2017). Government Decision 3270, Merging the National Cyber Directorate .

vital national, security goal and a national interest vital to its national security."[7] In 2016 the transfer of responsibility for "vital computerized systems" to the National Cyber Organization was arranged in accordance with the Regulation of Security in Public Entities Law (1998), in which the Directorate is specified as the instructor of various systems and organizations, including maritime companies and infrastructures (Ashdod Port Company, Haifa Port Company and Petroleum & Energy Infrastructures Ltd.).[8]

Operational Technology in the Sea Ports

There are, on average, 332 central OT computerization systems in a sea port, which are based on a variety of vendors, operating systems, and applications. This operational technology serves as an interface linking man and machine, thereby assisting in performing the critical functions. The maritime operational technology is unique in that this technology is based on obsolete operating systems such as Windows XP/7, and most of them nowadays are no longer supported by Microsoft[9] and security updates are no longer released. Most of the OT systems are not permanently connected to external networks, most of them do not have protective and defensive systems installed, such as antivirus, and if such are installed, they are usually out of date, which complicates maintenance and constitutes cybersecurity vulnerabilities.

Figure 1 below presents the deployment of the operational systems in a sea port such as: various cranes such as Rubber Tyred Gantry cranes (RTG), which arrange the containers inside the port grounds, and Ship To Shore cranes (STS), which load and unload containers from ships at an average speed of 26 moves per hour, transport vehicles, the system for routing and managing the maritime picture, breakers, gates and portside vessels. These systems operate on separate networks, which among them use "Ethernet", "Serial" communication and also wireless communication, which transfers data (loading or unloading plans and operation and maintenance instructions) from the port control center (Terminal Operating System – TOS) to a wide range of internal and external port systems.

---

7 Prime Minister's Office, Israel (2015). Government decision 2443, Advancement of National Regulation and Government Cybersecurity Leadership [Hebrew]; Prime Minister's Office, Israel (2015). Government decision 2444, Advancement of National Preparedness for Cybersecurity.

8 Israeli Knesset (2017), Center for Research and Information, Regulating the Responsibility for Cybersecurity in the Government and in Public Bodies.

9 Microsoft, Support for Windows XP ended; Microsoft, Support for Windows 7 ended

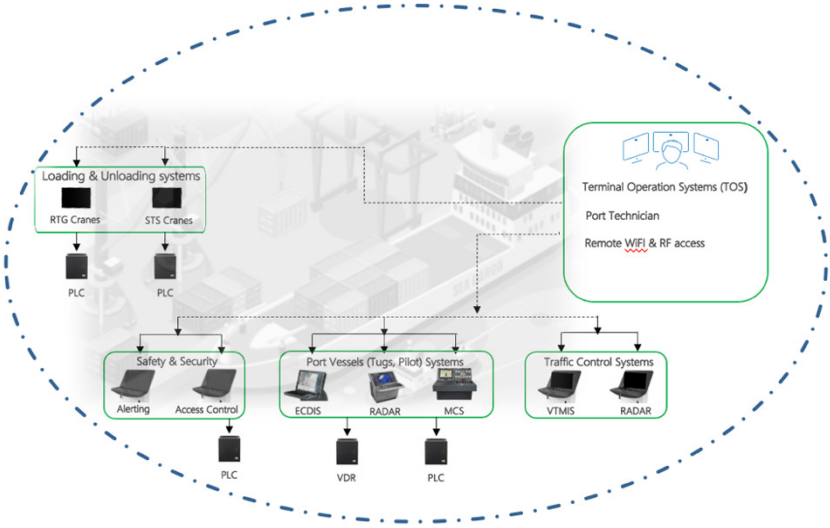

Figure 1: Deployment of main OT systems in a sea port

Operational technology system attack vectors

There are two types of vectors that attackers use to penetrate and damage OT systems in the maritime working environments and particularly in the sea ports. One is the External Attack Vectors. These vectors find the vulnerabilities of the information network, which the attacker exploits in order to insert the attack code from the external information systems into the internal operational technology systems. The attacker does this by using various techniques such as manipulations and deceit. In sea ports, the threat of using an external attack vector in order to harm operational systems is significant because the port has many interfaces with external bodies with different characteristics. In many cases, the information network is connected directly to the Terminal Operating System, which is connected to the operational network. Also, some of the everyday communication with the port operational systems are based on WiFi and RF networks, which are exposed to takeover and abuse as a vector for penetrating the operational network. The second kind of attack vector is the Internal Attack Vector, where users with access rights use the OT systems, such as crew members, technicians and other service providers, who in most cases unwittingly perform routine actions, thereby inserting the attack code from the external information network into the internal network and into the OT systems themselves.

Figure 2 below illustrates the internal attack vectors and the insertion points from the information network into the operational system in the port. For example, the port technicians and the system manufacturers routinely perform remote maintenance of the operational systems via cellular communication, RF and WiFi, or locally on the systems by connecting a computer or detachable memory device (USB). In doing so, they insert the attack code from the IT system into the OT system, which spreads to the rest of the OT systems.

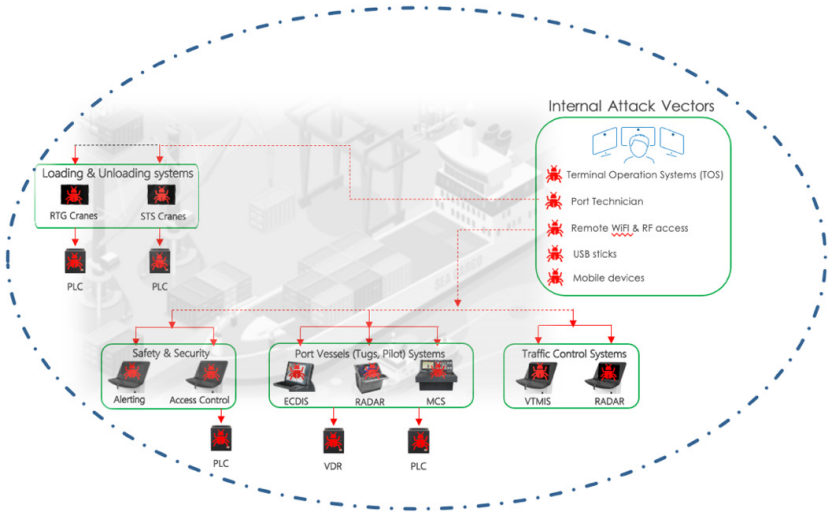

Figure 2: Internal attack Vectors in the port and the spread of the attack to all OT systems

Defense Approaches

In protecting the operational systems in the sea ports, two main approaches can be defined: the 'Outside-In' defense approach (which is now common in sea ports), which defines the external attack vectors as the main threat with which it has to contend, and the 'Inside-Out' defense approach, which provides a protection solution to both the external and internal attack vectors.

The defense approach which is based on '**Outside-In**' technology defines the external attack vectors as the main threat with which it has to contend. In this approach, the coping strategy is similar to installing fences around a secured site. It copes with the cyber threat through the use of a variety of technologies originating from protection of IT systems, such as deployment of a firewall, which prevents entry of unwanted communications into the organizational internal network. Installation of antivirus and disarm systems, which scan files before using them and which issues an alert

to the user upon detection of a malicious file with a recognized signature based on a list which gets updated from time to time. Efficient use of antivirus programs requires a continuous Internet connection, or routine updating of the new malicious file signatures. Without these updates, the effectiveness of the antivirus diminishes considerably. Another technology is network monitoring, which requires sensors to be deployed at various points throughout the network. Its main goal is to detect and alert on irregular network activities. These systems usually require a control center and a human factor to supervise and respond when necessary. This technological concept has several weaknesses: exposure to human error, false alarms, mistaken diagnosis, analyst burnout and a real difficulty in protecting operational systems against the threat of internal attack. These vulnerabilities may lead to a situation where malware succeeds in penetrating the operational network, and from there it can propagate to all of the OT systems. Quite often, these attacks penetrate the OT systems without the users' knowledge, and only months later and at a specific timing will they be activated, causing considerable damage without being able to respond.

A defense approach based on '**Inside-Out**' technology focuses on implementation of an active preventive protection technology in each one of the OT systems throughout the port, thereby delivering a protective solution to both attack vectors (the external and the internal), by implementing protective layers with various capabilities which enable protection, detection and alerting in three dimensions: EXE files, communication, and devices. All of this is done on each one of the OT computerization systems in the port. This approach does not require routine updates, it does not require the users to be trained or to have any pre-existing cyber knowledge, a connection to the Internet or a list of updated malware signatures. It is suitable for protecting both legacy and new systems or whether or not these are connected to the network. It enables the manufacturers and the technical personnel secure remote installation and maintenance, it enables the port operators to present a secure, up-to-date situation status of the cybersecurity on each one of the OT systems and it is therefore more suitable for protecting the OT systems operating in the sea ports.

In fact, the main difference between the two defense approaches is that in the 'Outside-In' approach, if the malware has succeeded in getting past the protection systems (the perimeter fence), it gains access to a large number of OT systems, all interconnected over internal networks and totally unprotected. On the other hand, in the 'Inside-Out' defense approach, the malware has got to attack each and every OT system separately, and even if it succeeds in penetrating one system, the damage is going to be localized only, and the recovery process will be shorter and much

easier. Figure 3 below shows the deployment of the protective software on all of the OT systems in a sea port.

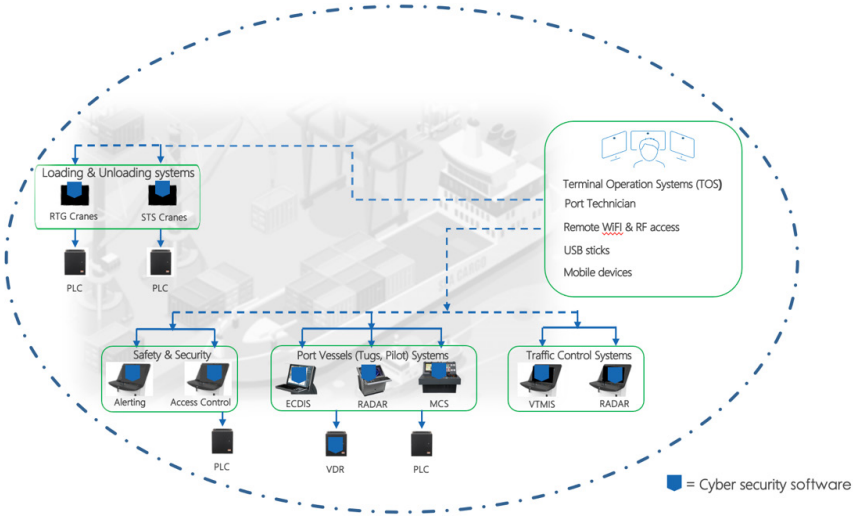

Figure 3: The 'Inside-Out' defense approach in a sea port

Threat cost analysis

A study done at Cambridge University will facilitate the analysis of a cyber threat to the Israeli ports. The study examined the impacts of three cyber attack scenarios on several large ports in the Asia-Pacific region. The researchers estimate that the damage from the worst-case scenario, codenamed "Shen Attack", of a cyber attack against approximately 15 ports in Japan, Malaysia, Singapore, South Korea and China, could incur losses of approximately $109.8 billion.[10] It described an attack through a computer virus which first attacks in a ship, spreads to the ports, and leads to severe disruptions and financial losses through the use of three severity levels, which are felt the world over due to the global connectivity of the maritime supply chain. The researchers estimate that an attack of this magnitude, which affects the sea ports, would inflict significant economic damage to a wide range of businesses due to reduced output and consumption, the costs of the response and the dimension of the supply chain. In a scenario which simulated an attack against nine ports, approximately 1,427,783 TEU were impacted for a period of between four and seven days until complete recovery. The direct financial damage (damage

[10] LLOYD'S (2019), University of Cambridge and Lloyd's, (2019). Shen Attack: Cyber risk in Asia Pacific ports.

to trade and businesses in the countries of the ports due to delays in deliveries) totaled approximately $36.8 billion and the indirect loss (damage to commerce and businesses in the countries with which the affected port has maritime trade relations due to delays in delivery) totaled approximately $19.1 billion, thus the total amount of the damage was approximately $55.9 billion.

The following assessment is based on the scenario of an attack on nine ports which is the more conservative scenario (the amount of financial damage per TEU was the lowest). It can be assumed that the average impact of a delay in the handling of one TEU would be equivalent to direct financial damage of $25.7 thousand (the quotient of $36.8 billion by 1,427,783 TEU), indirect financial damage of approximately $13.3 thousand (the quotient of $19.1 billion divided by 1,427,783 TEU), and to approximately $39.1 thousand (the quotient of $55.9 billion divided by 1,427,783 TEU). Based on these assumptions and referring to a cyber threat as a country-level threat according to the DNV definition (targeted cyber attacks using sophisticated means, abundant resources, good technical capabilities, good knowledge of the systems and a high level of motivation),[11] the damage that can be caused to the four Ports of Israel (Ashdod, Haifa, Israel Shipyards and Eilat) can be estimated. With a GDP of approximately $370.2 billion in 2018,[12] we can calculate the number of TEU's handled in Israel per day (the quotient of 2,940,917 TEU divided by 365 days),[13] we get a result of 8,057 TEU and we multiply by the number of days of the business disruption due to the cyber attack (multiplying 8,057 TEU by four days and seven days) and we get a number equal to 32,228 TEU as a minimum, and 56,399 TEU as a maximum, which were impacted by the cyber attack. To calculate the direct damage, we multiply by $25.7 thousand (the value of the direct damage per TEU unit) and we get the minimum direct damage of $828.2 million, and a maximum direct damage of $1.4 billion. To calculate the indirect damage, we multiply by $13.3 thousand (the value of the indirect damage per TEU unit) and we get the minimum indirect damage of $428.6 million, and a maximum indirect damage of $750.1 million. To calculate the total damage, we multiply by $39.1 thousand (the total value of the damage per TEU unit) and we get the minimum total damage of $1.2 billion, and a maximum total damage of $2.2 billion.

11 IUMI (2018), DNV GL releases first cyber security class notations.

12 The World Bank, UNCTAD, World Bank national accounts data, and OECD National Accounts data files.

13 The World Bank, UNCTAD, Container port traffic.

Response cost analysis

To estimate the cost of the response to the maritime cyber threat, taking into consideration the complexity of estimating the threat cost, the difficulty in proving loss, the appropriateness and the ways of implementing the various solutions, methods were examined for recognizing assets, their value to the organization, the threats, their impact, technological vulnerabilities, the probability and the need to select a risk mitigation strategy.

Jerman-Blažič (2008) compared the cost of the threat to the cost of the response and estimated that the optimal investments in information security is roughly 36.8% of the potential loss emerging from the threat. Srinidhi et al. (2015) point out that managers have incentives to invest more in cyber security than investors, and how cyber insurance minimizes over-investment on the part of managers in specific assets in favor of improving the cyber security. Wang (2019) suggests an innovative insurance model based on cyber threat-adjusted coverage with emphasis on the Risk Assessment sharing in the investment in security.

So far, most of the efforts to deal with the maritime cyber threat in general, and in the sea ports in particular, and to estimate the resulting costs – have focused on the insurance aspects and on monitoring, risk management and training solutions. Less estimation work has been done on solutions based on a technology-based 'Inside-Out' defense approach and on what is the cost of the protection required in order to significantly mitigate the cyber threat on the sea ports.

Table 1: The costs of the solution in US dollars[14]

	Total quantity	Number of operational systems in a single Port	Average operational systems in a single Port	Annual cost of protecting one operational system in US dollars	Annual cost of protecting a single Port in US dollars	Annual cost of protecting all the Ports in US dollars
Sea ports in Israel	4	77–586	332	300–5,500	99.6 thousand 1.82 million	398.4 thousand 7.3 million

Cost comparison: threat versus solution

To help decision-makers in the field of risk management of cyber threats to the sea ports in Israel, table 2 shows the costs of the threat versus the costs of the solution for protecting the sea ports in Israel. The comparison is presented in percentages, and within that taking into consideration the optimal investment in

[14] Proven Data (2020), How Much Does Cyber Security Cost? Common Cyber Security Expenses & Fees.

protection, approximately 36.8 percent of the cost of the cyber threat, as defined by Jerman-Blažič (2008). The table data clearly indicates that the cost of the solution for protecting against the maritime cyber threat to the sea ports in Israel is significantly lower than the definition of the optimal percentage of investment in defense. This is given that the most expensive cost of the protection solution (annual cost of approximately 5,500 dollars for protecting one operational system) for Israel's ports totals approximately 0.88 percent of the cost of the direct threat, and approximately 0.6 percent of the total cost of the threat.

Table 2: Costs of the threat versus costs of the solution

Asset type	Cost of direct threat in US dollars	Total cost of threat in US dollars	Cost of solution per year in US dollars	Difference in percentages versus direct cost of threat per year	Difference in percentages versus overall cost of threat per year	Low cost of direct/ total damage versus high cost of protection in percentage points
Sea ports in Israel (4)	828.2 million 1.4 billion	1.2–2.2 billion	398.4 thousand 7.3 million	0.028–0.88	0.018–0.6	Direct 0.88 Overall 0.6

Conclusion and Insights

As a consequence of the technological development in sea ports, the connectivity, threat complexity and the strategic importance of the sea ports to the State of Israel's security and economy, decision-makers (port managements and regulators) should evaluate the existing cybersecurity approaches and their costs.

The findings of the calculated analysis indicate that the cost of the solution to the threat of one cyber attack on Israel's four sea ports is less than a quarter of one percent of the cost of the threat itself. In view of this, it is advised to consider adopting the 'Inside-Out' defense approach through implementation of multi-layered cybersecurity solutions, which are compliant with the protection standards against a state-level threat, thereby enabling the sea ports in Israel to mitigate the security gaps. At the same time, state incentives must be created, the regulation has to be adapted and the responsibility for coping with the cyber threat to the sea ports' operational technology systems must be shifted from the human factor to active technological solutions.

Sources

Arslan, V., Kurt, R. E., Turan, O., & De Wolff, L. (2016). Safety culture assessment and implementation framework to enhance maritime safety. *Transportation Research Procedia*, 14, 3895–3904.

Jensen, L. (2015). Challenges in maritime cyber-resilience. *Technology Innovation Management Review*, 5(4), 35.

Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, 28(5), 413–422.

Luo, M., & Shin, S. H. (2019). Half-century research developments in maritime accidents: Future directions. *Accident Analysis & Prevention*, 123, 448–460.

Pomeroy, R. V., & Earthy, J. V. (2017). Merchant shipping's reliance on learning from incidents–A habit that needs to change for a challenging future. *Safety Science*, 99, 45–57.

Rid, T., & McBurney, P. (2012). Cyber-weapons. *RUSI Journa*l, 157(1), 6–13.

Rose, A., Prager, F., Chen, Z., Heatwole, N., & Warren, E. (2017). Economic Consequence Analysis of Disasters: The E-CAT Software Tool. Springer

Schauer, S., Stamer, M., Bosse, C., Pavlidis, M., Mouratidis, H., König, S., & Papastergiou, S. (2017). An adaptive supply chain cyber risk management methodology. In *Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL)*, vol. 23 (pp. 405–425). Berlin: epubli GmbH.

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems*, 75, 49–62.

Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, 57, 101173.