International Journal of Advanced Smart Convergence Vol.11 No.3 7-16 (2022)
http://dx.doi.org/10.7236/IJASC.2022.11.3.7

IJASC 22-3-2

Summary of Maritime Cyber Attacks and Risk Management

Mohammed Abdulhakim Al-Absi[1], Ahmed Abdulhakim Al-Absi[2], Ki-Hwan Kim[3], Young-Sil Lee[3], Hoon Jae Lee[4]

[1]Dr, Department of Computer Engineering, Dongseo University, Busan, Korea
[2]Associate Professor, Department of Smart Computing, Kyungdong University, Korea
[3]Assistant Professor, International College, Dongseo University, Busan, Korea
[4]Professor, Dongseo University, Division of Information and Communication Engineering, Busan, Korea
E-mail mohammed.a.absi@gmail.com, absiahmed@kduniv.ac.kr, ghksdl90@gdsu.dongseo.ac.kr, lys0113@gdsu.dongseo.ac.kr, hjlee@dongseo.ac.kr

Abstract

The targets of cyber-attacks are not limited to the websites and internal IT systems of shipping agencies. Ships and ports have become important targets for cyber attackers. This paper examines the current state of ship network security, introduces the International Maritime Organization's resolution on ship network security management, and summarizing the cyber-attacks in maritime so the readers can have a general understanding of maritime environment.

Keywords: *Ship Cyberattack, Security; Risk Awareness; Risk Management; IMO.*

1. Introduction

ship-shore information integrated network system fully considers the characteristics of ship-shore communication and utilizes the existing global satellite network and communication resources to transmit information cost-effectively, quickly, safely, and accurately. According to the characteristics of ship-shore communication, the network architecture of ship-shore information integration system is mainly composed of three levels: ship network information platform, ship-shore communication system, and shore-side network information platform. The data exchange between the ship network information platform and the shore-side network information platform is realized through the ship-shore communication system [1].

Data Acquisition and processing system can be divided into tow layers network structure, the upper layer is Ethernet, and the lower layer is fieldbus network. The upper layer network adopts a ring redundant Ethernet network structure, and the network is connected to the workstations that realize human computer interaction and the database servers that perform data storage and processing[2]. The network topology structure of the lower network is mainly adopting the fieldbus mode, and the data acquisition module and the communication module are connected to the network which are used for the collection, analysis and processing of the filed

Manuscript Received: June. 14, 2022 / Revised: June. 18, 2022 / Accepted: June. 22, 2022
Corresponding Authors: lys0113@gdsu.dongseo.ac.kr
Tel:*** - **** - **** Fax: +82-51-320-4248
Assistant Professor, International College Dongseo University, Busan, Korea

data. The data conversion communication between the two-layer networks is mainly realized through the gateway. The gateway is the core of the data transmission system [3]. It is mainly responsible for analyzing, processing, and summarizing the data collected by the lower data network and forming a data stream according to a certain format and storing it in the database server. The processed data can be transmitted to the shore-based application system of the ship operating company through the ship to shore communication equipment, which is convenient for monitoring the operation and usage of the ship. In addition, these data van also be transmitted in real time to the network clients of the captain, chief engineer, and the crow in duty through the ship wide network information system, so that the crew can monitor the important monitoring point of the ship in real time in the room [4].

Shore based application management system: The shore-based application system platform is the core of information processing and decision support for shipping enterprises. After the ship data enters the shore-based network information platform through the ship shore communication system, the data server will first perform data verification and intelligent splitting, and then write the data into the relevant database [5]. The shop data and all other related data will finally be collected in the shore-based network information platform, and the data will be called by different clients and the ship operation data will be delivered to the shore-based management personnel in timely and accurate manner and the shore-based management personnel can also pass this. The system sends the latest information and company instructions to the ships in operation so that the operating company can better control the operation status of each ship[6].

Ship shore communication system: For a long time, data sharing and exchange between ships and shores of shipping enterprises has been a big technical problem. In the early says, people used the ay of mailing disks to transmit relevant data information without any timeliness. With the development of existing information network and communication resource technology, people are constantly looking for reliable ship shore communication technology to realize fast, safe, reliable and accurate information transmission [7].

The ship shore communication system adopts different communication equipment according to different use environments and use requirements [8]. The well-known shop shore communication equipment includes maritime satellite INMARSAT-F station (INMARSAT-F provide a high-speed, high-quality communication environment on ships [9]), INMARSAT-C station (A two-way store and forward system, Inmarsat-C and Mini-C transmits communications from ship to ship, ship to shore, and shore to ship. Data transmission and reception includes telex, email, chart updates, SMS, and weather updates [10]), telecommunication network and so on.

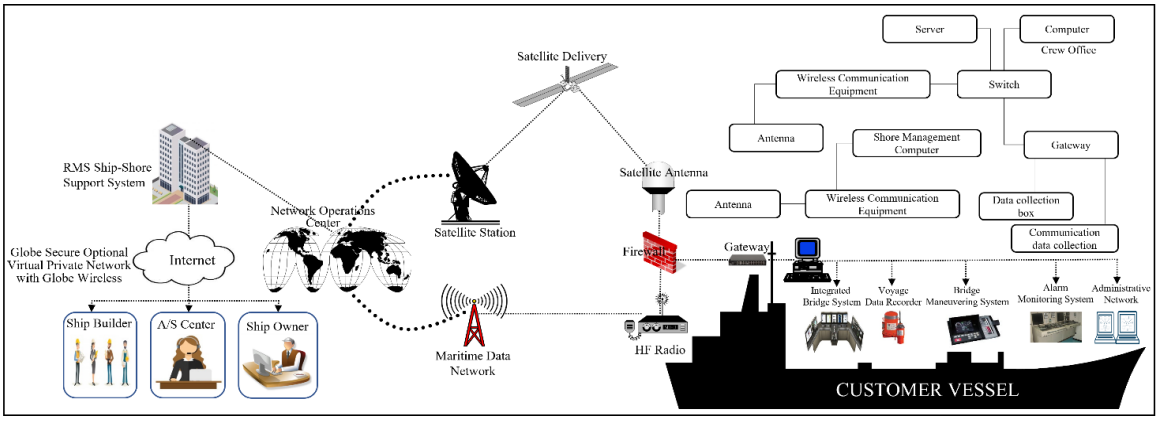

Figure 1. Ship to shore integrated monitoring system

To realize the ship- shore integrated monitoring system to manage, the stability, safety and timeliness of the ship-based acquisition and processing system must be ensured first. The system requires the ship to establish an independent ship local area network and connect with the ship communication ship server. On the basis of collecting signals, the data is packaged to the ship satellite communication equipment through the communication ship server and sent to the satellite ground station through the maritime communication satellite.

The mail processing center of the shore-side network information platform will scan in real time, and after receiving the ship data package, it will automatically distribute the special mailbox for ship data, and the application server will perform data verification and intelligent splitting, and according to the content of the data package, the data will enter the shore. The terminal server display platform displays, if necessary, it can be directly written into the ship dispatching system database by using CONNECT technology. The whole process is smooth and concise, fast, efficient, and cost-effective. In the same principle, shore-side data can reach designated ships, so as to realize the exchange and synchronization of ship-shore data and achieve the goal of ship-shore information integration. The ship's network information platform and the shore-side network information platform are independent, but also connected to each other through the ship-shore communication system, highlighting the characteristics of system

The very-high frequency band, medium-wave band, and short-wave band are mostly used for wireless communication between ships and shore or between ships. According to Global Maritime Distress Safety System (GMDSS) of the International Maritime Organization (IMO) [11], the maritime zones in which ships operate are divided into four categories, ranging from A1 to A4, and each category calls for the installation of the appropriate radio equipment as shown in Table 1.

Table 1. Maritime zones

				
Device				
Communication Coverage	37.04-55.56Km	740.8Km	within 70 degrees north and 70 degrees south and is within INMARSAT satellite	Worldwide
Technology	VHF-MF/DSC	MF/DSC	INMARSAT /HF	EPIRB/HF

A1 is the short distance area between 20 and 30 nautical miles(nm) from the nearest coast station, general communication, distress/safety communication, search and rescue operations, and on-site use by digital selective calling devices (DSC) and radiotelephones using the frequency of the very high-frequency band are all included(Ch. 70/156.525 MHz) [12]. A2 is the medium distance sea area about 150 nautical miles(nm) from

the coast and includes distress/safety communication, radiotelephone, general communication, rescue and search by DSC, and narrow-band direct printing telegraphs (NBDP) are carried out on a regular basis. Long range coverage areas apply to ships in open sea, radiotelephones, and terrestrial radio communications are provided by DSCs, NBDPs in the shortwave range for distress/safety communications, general communications, and rescue and search operations. High-frequency communication is an important radio communication method especially for ships navigating in the sea area A4 outside the Inmarsat satellite communication area A3.

From Figure1, A1 and A2 refer to the large, intricate portions of each country where tiny ships or boats float. The sea areas A3 and A4 are the oceans where the ships float. Different radio connection required vessels to have on board depend on the region of operation of that vessel.

2. Guidelines for Maritime Cyber Risk Management

The development of technology brings clear benefits, but also introduces cyber risk into the maritime industry. In 2017, the International Maritime Organization adopted resolution MSC.428 (98) entitled "Security Management System: Maritime Cyber Risk Management", which encourages management companies to establish a ship cyber risk management system and incorporate it into the ship safety management system [13].

The "Guidelines for Maritime Cyber Risk Management" issued by IMO put forward high-level recommendations for maritime cyber risk management and provide guarantees for maritime transport to cope with the current urgent cyber dangers and vulnerabilities [14]. The guidelines introduce the relevant basic concepts related to maritime cyber risk, point out the main systems at all levels that are vulnerable to attack on board, put forward management requirements, and point out several functional elements for establishing effective cyber risk management [15]:Table 3 shows the maritime cyber risk management.

Table 3. Cyber Risk Management Approach

Cyber Risk Management Approach	
Identification	Define personnel roles and responsibilities. Inventory the ship's equipment that may be exposed to cyber-attacks, distinguish information technology systems from operational technology systems, and identify systems, equipment and data that may interfere with ship operations and cause risks.
Protection	Strengthen the daily network security management, reduce the vulnerability caused by the unintentional behavior of the crew, reduce the probability of network incidents, and achieve the purpose of preventing network risks.
Detection	Establish detection procedures to detect the occurrence of network events in time.
Response	Establish a cyber risk emergency plan to deal with ship cyber security incidents.
Recovery.	Backup regularly. Recovery of corrupted data after a cyber incident.

Data products depend on data product specifications, and data product specifications rely on the S-100 data model. As the S-100 data model stabilizes, there are currently more than 20 data product specifications registered and under development by domain managers in S-99. , see Table 4 [16].

Product Numbers	Specification	Develop Organization
S-101	Electronic Navigational Chart	IHO
S-102	Water Depth Surface	IHO
S-103	Underwater Navigation	IHO
S-104	Water Level Information	IHO
S-111	Surface flow	IHO
S-121	Maritime Limits and Boundaries	IHO
S-122	Marine Reserve	IHO
S-123	Radio Services	IHO
S-124	Navigation Warning	IHO
S-125	Navigation Service	IHO
S-127	Maritime Traffic Management	IHO
S-128	Catalogue of Nautical Products	IHO
S-129	Under Keel Clearance Management	IHO
S-131	Marine Harbor Infrastructure	IHO
S-201	Aids to Navigation Information	IALA
S-210	Inter-VTS Exchange Format	IALA
S-211	Port Call Message Format	IALA
S-212	VTS Digital Service	IALA
S-230	AIS Application Specific Messages	IALA
S-240	DGNSS Station Almanac	IALA
S-245	eLoran ASF Data	IALA
S-246	eLoran Station Almanac	IALA
S-247	Differential eLoran Reference Station Almanac	IALA
S-401	IEHG Inland ENC	IEHG
S-402	IEHG Bathymetric Inland ENC	IEHG
S-411	Ice Information	WMO Service Commission
S-412	Weather and Wave Hazards	WMO Service Commission
S-413	Weather and Wave Conditions	WMO Service Commission

S-414	Weather and Wave Observations	WMO Service Commission
S-421	Route Plan	International Electrotechnical Commission
S-501	Military	Working Group

3. Maritime Cybersecurity:

The information technology (IT) domain includes systems in ports, offices, and oil rigs, while operational technology (OT) covers a variety of uses such as related navigation systems, systems and controlling engines, cargo management...etc. These systems weren't linked to any shore-based systems a few years ago, and they were isolated from one another. However, in recent years, the OT and IT sectors have been able to intersect because to the advancement of digital communication and technology [17].

Ransomware attacks are a growing problem for the maritime industry. Table 5 shows the summary of Maritime cyber-attack.

Table 5. Summary of Maritime cyber attack

Reference	Type	Year	Description and Location
[18]	Malware	23rd-May-2022	The Port of London Authority (PLA) was hacked and knocked its website offline.
[19]	Ransomware Attack	18-May-2022	Carriers respond to cyber-attack in Costa Rica (Central America). Ransomware cyber assaults on Costa Rican institutions have prompted emergency measures across the shipping industry, since imports and exports have been severely impacted.
[20]	Phishing Attack/ Ransomware Attacks	23-Fab-2022	Jawaharlal Nehru Port, Cyber-attack of the management information system (MIS) has affected the container terminal run by the port authority India. The port authority has yet to make a statement regarding the attack.
[21]	Ransomware Attack	25-Nov-2021	"Unauthorized access to its IT systems" occurred at Swire Pacific Offshore, a Singapore-based shipping company. While the Singapore-based corporation claims the hack "has not meaningfully impacted worldwide operations," data and security specialists think the attack was carried out by a well-known cyber gang and resulted in a large loss of data, including critical corporate and employee information.
[22]	Ransomware attack	20-Sep-2021	A data breach has been reported by CMA CGM, a French shipping company. Customers' names, email addresses, phone numbers, and job information were leaked, according to a security advisory issued by the container transportation and marine company located in Marseille (France).
[23]	Ransomware	27-July 2021	Transnet, the main South African logistics, rail, and port company, was also targeted. The incident looked to be caused by ransomware, but the organization provided many details.

[24]	Malware	March/July-2021	In Japan, the Tokyo-headquartered shipping giant was hit by a malicious cyber-attack in March. The second incident, which occurred in July, was described as involving “unauthorized access to overseas subsidiary systems.
[25]	Phishing Attack/ Ransomware Attacks	June-12-2021	South Korea’s national flagship carrier HMM has fallen victim to a cyber-attack that has mainly impacted the company’s email server.
[26]	Ransomware Attack	20-Nov-2020	The port of Kennewick in (United State), learned that it had fallen victim to a digital ransomware attack, in which cybercriminals circumvented its systems, placed a sophisticated encryption lock on the port’s servers, and demanded $200,000 ransom to restore access to the port's servers and files. A differentiated cyber attack that uses advanced military grade encryption to exploit ransomware by focusing on port-locking servers and taking those servers hostage.
[27]	Ransomware Attacks	11-June-2020	Norwegian shipbuilder Vard (Romania), servers was hit with an encryption cyberattack where the attack affected Vard’s shipyard by a data breach. The accompany didn’t want to comment more about the because it is complex matter.
[28]	Ransomware Attacks	May-2020	Cyber-attack targets port near Strait of Hormuz (Iran). A cyber-attack managed to damage a number of private systems at the Shahid Rajaei port.
[29]	Malware attack	10th-April-2020	In Switzerland, Mediterranean Shipping Company (MSC) has confirmed that a malware attack caused a data center outage which led to its main customer facing websites being down for several days.
[30]	Ransomware Attacks	March-2020	In France, the port of Marseilles was the next to be targeted, Mespinoza/Pysa. Maritime infrastructures were not directly targeted in this case but were harmed as a result of their interaction with information systems in Aix-Marseille-Provence, which was the attack's principal objective. After few weeks from this attack, company has made a clear report regarding this attack.
[31]	Phishing Attack	5-Nov-2019	In UK, Marine firm James Fisher reports cyber breach. hackers had gained unauthorized access to its computer systems, sending its shares down as much as 5.7%.
[32]	Malware Attack	8th-July-2019	U.S. Coast guard issues alert after ship heading into port of New York hit by cyberattack.
[33]	Ransomware	25-Sep-2018	The port of San Diego in the United States suffered from cyber-attacks. The Port of San Diego suffered a ransomware attack that damaged its internal IT systems.
[34]	Ransomware	20-Sep-2018	Port of Barcelona in Spain. The cyber-attack on the Port of Barcelona did not affect ships entering or leaving the port, only internal IT systems were affected.
[35]	Ransomware Attacks	8-June-2018	US officials told the Washington Post, Chinese government hackers steal data include plans for a supersonic missile project from US Navy contractor.

4. Conclusion

To give readers a comprehensive overview of the maritime environment, this article provides a summary of cyber-attacks in the maritime environment. According to the Great Disconnect Report, there is a gap between IMO preparedness and reality when it comes to responding to cyberattacks. Senior employees are less likely

to be aware that their company has been the victim of a cyberattack, whether they are onshore or offshore. In fact, 26% of maritime employees do not know what to do in the event of a cybersecurity crisis, and 32% do not regularly practice cybersecurity. In the onshore sector, 38% of senior executives do not know or have their company's cybersecurity strategy. Among the report's key findings, 52% of industry professionals believe their company has a process in place to capture cyber threat intelligence. According to the report, 44% of industry professionals said their company had been the target of a cyberattack in the past three years. In the past three years, 36% of business professionals believe their company has been the victim of a cyberattack. 73% of respondents said their company has a plan in place to deal with cybersecurity incidents. In 3% of cyberattacks, respondent companies paid a ransom. On average, $3.1 million in ransom was paid. 4% of business professionals in this sector believe their company has insurance against cyberattacks. Maritime cyber risk refers to the destruction, loss or leakage of technical information or systems that compromise the security of shipping-related operations and jeopardize shipping assets. Meanwhile, the shipping industry has recognized the risks that can arise from the digitization and interconnectivity of ships, and the topic of ship cyber security has led to extensive discussions at IMO conferences in recent years.

Acknowledgement

This work was supported in part by the Ministry of Education, Science and Technology, Basic Science Research Program, through the National Research Foundation of Korea (NRF), under Grant NRF-2016R1D1A1B01011908. and was a part of the project titled 'Marine digital AtoN information management and service system development(2/5) (20210650)', funded by the Ministry of Oceans and Fisheries, Korea.

References

[1] OneOcean, “The Importance of Ship-to-Shore Communication Is More Vital Than Ever,” The Maritime Executive, Jun-2-2022 https://www.maritime-executive.com/features/the-importance-of-ship-to-shore-communication-is-more-vital-than-ever

[2] Liu, Sheng et al. “Ship information system: overview and research trends.” *International Journal of Naval Architecture and Ocean Engineering* 6 (2014): 670 - 684.

[3] E. Ouzounoglou, M. Koutsokeras, P. Bpye et al. “A multisource communication gateway and An advanced visualization interface for maritime surveillance systems based on the inter-VTS Exchange Format Service,” *International Journal of Transport Development and Integration*, Vol. 3, No. 4 (2019), 355–368

[4] Martin Sovind Jensen, “Insatech Marine Performance Monitoring System,” InsaTech, 01-07-2022 https://www.insatechmarine.com/products/performance/performance-monitoring-system

[5] I. S. Jang, M. S. Kim, “Implementation of the Shore-based Maritime Information Service Platform for e-Navigation Strategic Implementation Plan, ” J . Navig. P ort Res. Vol. 39, No. 3 : 157-163, June 2015

[6] “How Vessel Reporting System Makes your Reporting Job Easier,” CyberLogitec, October-13-2014 https://www.cyberlogitec.com/news/how-vessel-reporting-system-makes-your-reporting-job-easier/

[7] “Ship to Shore Communications” BATS, 27-06-2022 https://www.extendingbroadband.com/aerial-tracking/ship-shore-communications-2/

[8] “The INMARSAT-F" is released,” Jun-2003 https://www.jrc.co.jp/eng/100th/event-single/event105/index.html

[9] J. Ward, “Inmarsat’s The Future of Maritime Safety Report 2022 tracks rise in vessel incidents,” Fathom World, June-7-2022 https://fathom.world/inmarsats-the-future-of-maritime-safety-report-2022-tracks-rise-in-vessel-incidents-during-covid-19-pandemic/

[10] INMARSAT-C, 02-07-2022 https://www.inmarsat.com/en/solutions-services/maritime/services/inmarsat-c.html

[11] “Global Maritime Distress and Safety System (GMDSS),” Federal communications Commission, April-8-2022

https://www.fcc.gov/wireless/bureau-divisions/mobility-division/ship-radio-stations/global-maritime-distress-and-safety

[12] Koshevyy, Vitaliy Mykhaylovych and Aleksandr V. Shishkin. "Standardization of Interface for VHF, MF/HF Communication Using DSC within Its Integration with INS in the Framework of e-Navigation Concept." *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, vol 13, No 3,pp. 593-596 Sept 2019

[13] "Maritime Cyber Risk Management In Safety Management Systems, " *MSC.428(98) - International Maritime Organization*, 16-June-2017 https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

[14] "Guidelines On Maritime Cyber Risk Management," *MSC-FAL.1/Circ.3/Rev.1, International Maritime Organization*, 14 June 2021 https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf

[15] Jaime Alvarez, "IALA Workshop On Cyber Security," *International Association of Marine Aids to Navigation and Lighthouse Authorities Association Internationale de Signalisation Maritime,* Report of the workshop on Cyber security, Nov-19-2021

[16] "S-100 based Product Specifications" *International Hydrographic Organization (IHO)*, 09-06-2022 https://iho.int/en/s-100-based-product-specifications

[17] K. Stouffer, M. Pease, C. Y. Tang, T. Zimmerman, V. Pillitteri et al. "Guide to Operational Technology (OT) Security," *National Institute of Standards and Technology (NIST)*, April-2022 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf

[18] Editorial Team, "Cyber-attack targets Port of London Authority," In *Cyber Security, SAFETY4SEA,* May-27-2022 https://safety4sea.com/cyber-attack-targets-port-of-london-authority/

[19] M. Bruno, "Cyber attacks on Costa Rica prompt action from carriers," In *Port Technology International*, May-18-2022 https://www.porttechnology.org/news/cyber-attacks-on-costa-rica-prompt-action-from-carriers/

[20] Editorial Team, "Terminal at India's top container port affected by cyber-attack," In *Cyber Security, SAFETY4SEA*, Feb-23-2022 https://safety4sea.com/terminal-at-indias-top-container-port-affected-by-cyber-attack/

[21] "Ransomware Attack on Swire Pacific Offshore Breaches Personnel Data," In *The Maritime Executive,* Nov-26-2021 https://www.maritime-executive.com/article/ransomware-attack-on-swire-pacific-offshore-breaches-personnel-data

[22] J. Haworth, "French shipping giant CMA CGM suffers data breach" In *The Daily Swing Cybersecurity news and views,* Sep-21-2021 https://portswigger.net/daily-swig/french-shipping-giant-cma-cgm-suffers-data-breach#:~:text=French%20shipping%20company%20CMA%20CGM,employment%20information%20have%20been%20leaked

[23] S. Shead, "South Africa port operations halted and workers reportedly put on leave after major cyberattack," In *CNBC,* Jun-27-2021 https://www.cnbc.com/2021/07/27/transnet-halts-port-operations-in-south-africa-after-major-cyberattack.html

[24] S. Chambers, "K Line apologises for second hacking incident this year," Splash247, July-2-2021 https://splash247.com/k-line-apologises-for-second-hacking-incident-this-year/

[25] N. H. Prevljak, "HMM hit by cyber attack" In *Offshore Energy*, June-15-2021 https://www.offshore-energy.biz/hmm-hit-by-cyber-attack/

[26] P.M.Staff, "Washington's Port of Kennewick hit by cyberattack," In *Professional Mariner Journal of the Maritime Industry*, Nov-20-2020 https://professionalmariner.com/washingtons-port-of-kennewick-hit-by-cyberattack/

[27] "Norwegian shipbuilder Vard has been hit by a ransomware encryption cyberattack," *CSN Cyprus Shipping News,* June-11-2020 https://cyprusshippingnews.com/2020/06/11/norwegian-shipbuilder-vard-has-been-hit-by-a-ransomware-encryption-cyberattack/

[28] J. A. Gross, "Cyberattack on port suggests Israeli tit-for-tat strategy, shows Iran vulnerable," In *The Times of Israel*, May-19-2020
https://www.timesofisrael.com/cyberattack-on-port-suggests-israeli-tit-for-tat-strategy-shows-iran-vulnerable/

[29] M. Schuler, "Suspecting Cyber Attack, MSC Reports Network Outage – Update," *gCaptain leader in maritime and Offshore News,* April-10-2020
https://gcaptain.com/msc-reports-network-outage-cyber-attack-cannot-be-ruled-out/

[30] P. Paganini, "Massive cyber attack hit the town hall of Marseille ahead local election," In *Security Affairs,* March-15-2020
https://securityaffairs.co/wordpress/99658/malware/marseille-city-massive-attack.html

[31] N. Z. Hussain, "Marine firm James Fisher reports cyber breach," In *Reuters News,* Nov-05-2019
https://www.reuters.com/article/us-james-fisher-cybercrime-idUSKBN1XF1SQ

[32] D. Winder, "U.S. Coast Guard Issues Alert After Ship Heading Into Port Of New York Hit By Cyberattack," In *Forbes Cybersecurity,* July-09-2019
https://www.forbes.com/sites/daveywinder/2019/07/09/u-s-coast-guard-issues-alert-after-ship-heading-into-port-of-new-york-hit-by-cyberattack/?sh=3d3a454641aa

[33] P. Paganini, "Port of San Diego hit by a cyber attack a few days after the attack on the Port of Barcelona," In *Security Affairs,* September-28-2018
https://securityaffairs.co/wordpress/76623/hacking/port-of-san-diego-attack.html

[34] "Barcelona port suffers cyber attack," In *PortSEurope News and Information,* Sept-20-2018
https://www.portseurope.com/barcelona-port-suffers-a-cyber-attack/

[35] E. Nakashima, P. Sonne, "China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare," In *National Security Washington Post,* June-08-2018
https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html