Tanker Industry is More Ready against Cyber Threats

Aybars Oruc, AMIMarEST, MIET
Piri Reis University
Istanbul, Turkey
orucaybars@gmail.com

Synopsis

Cyber security in the maritime industry became crucial due to both academic researches and incidents. There are academic studies that show vulnerabilities in various navigation equipments such as GPS, ECDIS, AIS and ARPA-Radar. Additionally, there are different cyber incidents around the world.

Developments in technology, autonomous ship projects, academic studies and cyber incidents in the sector put in action IMO. As per ISM Code, all shipping companies are mandatory to add "Guidelines on Maritime Cyber Risk Management" manual to their SMS manuals until 01st January 2021.

Both OCIMF and CDI failed to be indifferent to developments that are important for tanker operators as well as IMO. While OCIMF added cybersecurity-related questions to vetting programs called TMSA 3 and VIQ 7, CDI also added cybersecurity-related items in SIR 9.8.1 edition.

On the other hand, RightShip provides significant vetting service for dry cargo ships. "Inspection and Assessment Report" is issued by RigthShip for dry cargo ships. Questions related with cybersecurity was added with Revision No: 11 dated on 11th May 2017 in "Inspection and Assessment Report".

In this study, cyber security related questions which are asked during TMSA, SIRE and CDI vettings which play a critical role for commercial life of tanker firms, were analyzed. Moreover, questions and efficiency of RightShip that offers vetting service for dry cargo ships, were assessed to maritime cyber security.

Also, cybersecurity-related questions in vetting questionnaires were interpreted by the author. These comments rely on benchmarking meetings among tanker operators where the author personally attended, and interview with key persons.

Noted observations during vettings may negatively impact both commercial life and reputation of the tanker operators. That's why the firm names and interviewee names were kept confidential.

In this study, it was seen that although IMO demanded verification of cyber security-related implementations for the ship operators until 01st January 2021, this process started earlier for tanker operators.

Keywords — maritime cyber security, tanker industry, vetting programmes, TMSA, SIRE, CDI, RightShip

http://doi.org/10.24868/icmet.oman.2019.030

1 Introduction

There are numerous accidents in the history of tanker transportation (Havold 2010). There are two well-recognized and non-profit organizations to decrease accidents, and increase the service quality in the maritime industry. These are OCIMF (Oil Companies International Marine Forum) and CDI (Chemical Distribution Institute).

They have their self-vetting programmes. SIRE (Ship Inspection Report Programme) and TMSA (Tanker Management and Self-Assessment) programmes were developed by OCIMF. OCIMF has important place in the maritime industry. Because “Consultative Status” was given to OCIMF by IMO. CDI which is another organization, provides vetting service for especially chemical tankers and gas carriers. These programmes also cause a competition among tanker operators.

OCIMF and CDI placed some criterias relevant with cyber security in their questionnaries. That’s why, tanker operators are forced to take actions related to cyber security due to TMSA, SIRE and CDI inspections. On the other hand, for dry cargo ships, it was seen that there are challenging vetting questions posed by RightShip. However, while OCIMF and CDI are non-profit organisations, RightShip’s private company status leads to questions about efficiency.

Some of researches and accidents regarding maritime cyber security are explained following headings.

1.1 Maritime Cyber Security Researches

There are numerous scientists and institutions researching vulnerabilities and attack methods belong to equipment on ships. Below, experimental cyber-attacks to various devices are explained.

1.1.1 GPS (Global Positioning System)

In 2013, researchers from University of Texas applied GPS spoofing attack to superyacht (LOA: 65m) called “White Rose of Drachs” and sheered this yacht from actual course. Fore of the yacht had GPS antenna. Stern part has spoofer RX antenna. Spoofer device processed signals from RX antenna and transmitted to TX antenna. GPS antenna of yacht confused these fake signals with real signals and deviated from course.(Bhatti & Humphreys 2014)

1.1.2 ECDIS (Electronic Chart Display and Information System)

When installed a malware, the attack can perform two kinds of actions: It can manipulate GPS coordinates via the network, and the malware can crash the operator station by provoking a bluescreen.(Lund et al. 2018)

1.1.3 AIS (Automatic Identification System)

An article published in 2014 reveals numerous vulnerabilities of AIS. These were categorised as Ship Spoofing, AtoN Spoofing, Collision Spoofing, AIS-SART Spoofing, Weather Forecasting, AIS Hijacking and Availability Disruption Threats.(Balduzzi et al. 2014)

1.1.4 ARPA-Radar (Automatic Radar Plotting Aids Radar)

In 2017, after receiving required permissions, Israel based Naval Dome firm, a series of cyber penetration test was conducted on various tankers, container ships, super yachts and cruise ships. As a result of these tests, radar was manipulated by using local Ethernet Switch Interface. Radar targets were eliminated, simply by deleting them from the screen. During this attack, radar did not give any alert or warning to attract attention of OOW.(Shefi 2017)

1.2. Maritime Cyber Attacks

Advancements in technology brings together cyberattacks. These attacks can be towards vessels, marine authorities and private companies. One of the vital points in marine clearly is jeopardising navigation safety of the ships.

1.2.1. Danish Maritime Authority (2012)

In April 2012, it was seen that Danish Maritime Authority was subjected to a cyber-attack, and this cyber-attack was announced to public in September 2014.(CyberKeel 2014)

It was seen that attackers want to obtain sensitive data about Danish shipping companies and merchant fleet. It was announced that this attack was highly sophisticated, it was state-sponsored and it is believed that this attack was organised by China. Chinese Embassy in Copenhagen refused all accusations, and announced that they had no knowledge about this attack.(The Local 2014)

1.2.2. South Korea (2016)

In April 2016, South Korea announced that around 280 vessels were under GPS jamming attack. By reason of this attack, affected vessels were forced to go back to port. It was claimed that this attack was organised by North Korea.(Graham 2017)

1.2.3. Maersk (2017)

On 28th June 2017, Maersk announced on the official website that they were under cyberattack by a virus called Petya(Maersk 2017). Maersk group's CEO Søren Skou stated that this attack on 27th June 2017 might have caused $200-$300 million financial losses to the company (Skou 2017).

1.2.4. Russia (2017)

On 22nd June 2017, a ship off Novorossiysk-Russia shore notified U.S. Coast Guard Navigation Centre about GPS. Coast off Novorossiysk-Russia, GPS screens of approximately 20 vessels showed incorrect location(Goward 2017). Experts claimed that this attack was organised by Russia to test defence system against American missiles(Goward 2017; Humphreys 2017)

1.2.5. German-Owned Container Ship (2017)

In February 2017, navigation system of a container ship with 8250TEU capacity that was controlled by hackers for 10 hours on route from Cyprus to Djibouti(Blake 2017).

1.2.6. Clarksons (2018)

British shipping services firm Clarksons announced on 30th July 2018 with a press statement that they were under cyber-attack. Company announced that this cyber-attack was between 31st May 2017 – 04th November 2017, and various personal data such as seafarers' personel informations, CVs, and financial data might be captured by hackers.(Clarksons 2018)

1.2.7. COSCO (2018)

On 24th July 2018, COSCO Shipping experienced a ransomware attack. This attack included U.S. offices of COSCO Shipping and COSCO's terminal at Port of Long Beach. COSCO's U.S. website, e-mail, phone and network infrastructure was affected from this attack.(WMN 2018)

2 Legislations and Vetting Programmes related with Maritime Cyber Security

There are various organisations whose decisions and applications are forceful, in the maritime industry. These organizations began to emphasise cyber security related topics after past incidents. IMO makes shipping companies assess cyber risks, and the rule enters into force as of 01st January 2021(IMO Resolution MSC.428 (98)). However, vetting companies acted quicker, and added cyber security related items to their inspection checklists.

2.1 Mandatory Regulation

ISM is an only mandatory code which is issued by IMO, regarding directly maritime cyber security.

2.1.1 ISM Code

Under ISM Code, all shipping companies are mandatory to add "Guidelines on Maritime Cyber Risk Management" manual to their SMS manuals until 01st January 2021.(IMO Resolution MSC.428 (98))

In compliance with ISM Code, for firms which have DoC (Document of Compliance), cyber security risk assessment will be mandatory as of 01 January 2021, and this assessment will be inspected in the first annual DoC verification following this date.

DoC means a document issued to a company which complies with the requirements of ISM Code.(ISM Code)

2.2 Non-Mandatory Vetting Programmes

2.2.1 SIRE

An essential vetting program developed by OCIMF is SIRE, and this program was launched in 1993. Aim of this program was to increase safety and quality standards on tankers. After vetting, inspection reports can be accessed by OCIMF members such as bulk oil terminal operators, port authorities, canal authorities, oil, power, industrial or oil trader companies which charter tankers/barges as a normal part of their business.(SIRE 2019)

SIRE inspections are conducted by SIRE inspectors on vessels. SIRE inspections have various questionnaires. Oil tankers, combination carriers, shuttle tankers, chemical tankers and gas tanker audits are conducted on VIQ (Vessel Inspection Questionnaire). The last edition is VIQ 7, and has 12 chapters. These are shown the Table: 1 below.

Chapter No	Topic
Chapter 1	General Information
Chapter 2	Certification and Documentation
Chapter 3	Crew Management
Chapter 4	Navigation and Communications
Chapter 5	Safety Management
Chapter 6	Pollution Prevention
Chapter 7	Maritime Security
Chapter 8	Cargo and Ballast Systems - Petroleum
	Cargo and Ballast Systems - Chemicals
	Cargo and Ballast Systems - LPG
	Cargo and Ballast Systems - LNG
Chapter 9	Mooring
Chapter 10	Engine and Steering Compartments
Chapter 11	General Appearance and Condition
Chapter 12	Ice Operations

Table 1: VIQ 7 Chapter List

VIQ 7 is effective as of 17th September 2018. It can be seen that in this edition, cyber security related questions are included in "Chapter 7: Maritime Security". These questions are listed below with the author's comments.

Question 7.14

Are Cyber Security Policy and Procedures part of the Safety Management System and is there a Cyber Response Plan onboard?

Author Comment

This question requires risk assessment related to cybersecurity, providing information about cyber threats, identifying key contacts, password management and mitigation measures.

In current inspections, inspectors first want to see if there is a plan. Risk assessment criteria do not challenge ship operators under current conditions. However, it is possible that inspectors will emphasise this topic over time. Some inspectors examine prepared plans in detail to make sure that these plans are created as ship specific.

Question 7.15

Are the crew aware of the company policy on the control of physical access to all shipboard IT/OT systems?

Author Comment

This criterion requires USB and RJ-45 port control on shipboard IT/OT systems. Thus, the main objective is to prevent virus infection on navigation equipment such as ECDIS.

This item is commonly interrogated during inspections. SIRE inspectors examine if USB ports and RJ-45 connections are under control. Precautions of companies are physically locking USB or RJ-45 portals or only permitting authorised devices and memory sticks to these ports by using cybersecurity software.

There are numerous hardwares with RJ-45 and USB ports from the bridge to the engine room in a ship. Although the secured status of all hardwares is not controlled by the inspectors yet, the secured status of USBs in equipment such as ECDIS, GPS, VDR are examined carefully.

Question 7.16

Does the company have a policy or guidance on the use of personal devices onboard?

Author Comment

This question examines if there is a procedure that prevents visitors on the ship (For example 3rd party contractors) to connect to ship network by using their personal devices such as crew smartphone, tablet and memory stick.

It is accepted that there are various visitors such as custom, agent, surveyor on ships. These individuals might be given with ship memory stick for special printouts. These memory sticks might contain virus, and this virus might infect the ship network and prevent IT/OT system to work in a reliable way. Declining printing on the ship side might lead to disruption in the operation. Therefore, this topic leads to discussions.

To meet these criteria, ship operators can provide an independent computer and printer from ship network, and allocate these devices only to 3rd parties. Ships without this system might want sending an e-mail to the ship and printing that e-mail.

Company procedures prohibit charging mobile devices such as crew and visitor's tablets and smartphones on USB ports.

Question 7.17

Is Cyber Security awareness actively promoted by the company and onboard?

Author Comment

This question examines raising awareness of the crew against cyber threats.

Inspectors observe existence of cyber security related posters on IT terminals. Posters known as “Social Media Guidance for Seafarers” or “Golden Rules” published by INTERTANKO are especially recommended. Additionally, it is recommended for the crew to watch cyber security related training videos, and keep these training records as evidence.

2.2.2 TMSA

Tanker Management Self-Assessment (TMSA) program is developed by OCIMF. Purpose of this program is to contribute tanker management firms to develop their Safety Management System (SMS). While SIRE and CDI are based on tankers, TMSA is based on auditing offices of tanker management firms. Companies give their answers to published questions. These answers are examined by TMSA experts via office audits. Office audits are not conducted periodically. Major oil companies such as Chevron, Shell and BP can demand for TMSA Office Audit, and conduct this audit. These audit takes approximately 2 days.

TMSA has 13 sections. These sections are called as “elements”. The elements of TMSA are shown the Table 2 below.

Element No	Topic
Element 1	Leardership and the Safety Management System
Element 2	Recruitment and Management of Shore-Based Personnel
Element 3	Recruitment, Management and Wellbeing of Vessel Personnel
Element 4	Vessel Reliability and Maintenance including Critical Equipment
Element 5	Navigational Safety
Element 6	Cargo, Ballast, Tank Cleaning, Bunkering, Mooring and Anchoring Operations
Element 7	Management of Change
Element 8	Incident Reporting, Investigation and Analysis
Element 9	Safety Management
Element 10	Environmental and Energy Management
Element 11	Emergency Preparedness and Contingency Planning
Element 12	Measurement, Analysis and Improvement
Element 13	Maritime Security

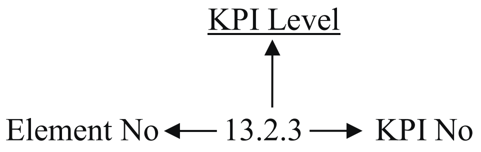
Table 2: TMSA 3 Element List

Questions are called as Key Performance Indicator (KPI). In TMSA, KPIs are divided into four levels. First level is basic, and forth level is the most advanced level. Firms that try to pass TMSA audit successfully, must meet the whole requirements of level 1 at least. Some charterers might require from tanker management companies to get higher TMSA level. That’s why, tanker firms try to meet highest level of requirements possible. In this way, the firms will have the opportunity to offer carrying service to a wider range in the maritime sector.

Before charter part agreements with MOCs (Major Oil Company), TMSA performance of tanker manager is reviewed. Depending on the type of charter party agreement, whole or partial KPIs in a certain level of TMSA can be required for tanker management company by MOC. Although it is not officially declared, according to charter party agreements of various MOCs, TMSA levels demanded from tanker management companies are listed below.(Karti 2017)

Level 1 → Tanker manager is satisfactory for V/C (Voyage Charter)
Level 2 → Tanker manager is satisfactory for CoA (Contract of Affreightment)
Level 3 → Tanker manager is satisfactory for T/C (Time Charter)
Level 4 → Tanker manager is satisfactory for a joint venture with a MOC

Element and level of a KPI can be easily understood from the code number. For example:



TMSA has been introduced to maritime sector in 2004. In 2008, scope and content were expanded with TMSA 2. On 10th April 2017, OCIMF published a guide for TMSA 3. This entered into force on 01st January 2018.

One of the most striking revisions in TMSA 3 is “Element 13: Maritime Security” which is new. This element has cyber security related KPIs at 2nd level, so that tanker firms were forced to take action regarding cyber security.

KPI 13.2.3
Policy and procedures include cyber security and provide appropriate guidance and mitigation measures.

Author Comment
This KPI expects risk assessment towards IT systems and technical and procedural precautions for these risks from ship operators.

Inspectors desire to analyse cybersecurity related company policies and procedures. Within policies and procedures, precautions for social media use is also analysed. Currently, there is no detailed analysis of risk assessment.

KPI 13.2.4
The company actively promotes cyber security awareness.

Author Comment
This KPI questions awareness of both crew and shore staff about cybersecurity. Social media use, secure password selection and controlled use of portable storage devices are inspected.

Inspectors might want to investigate training related recordings. Additionally, familiarity of the office personnel can be tested and inspected with different methods. For example, according to senior manager of a tanker operator firm, after an inspector in the office to inspect TMSA completed the inspected, the inspector asks to give a memory stick to an office staff to print the report. Office staff declines the request of the inspector by stating that USB drive cannot be connected to office computers due to technical precautions. Later, the inspector says that this was a trick to assess staff's awareness about cybersecurity.

2.2.3 CDI Ship Inspection

CDI is a non-profit organization. Inspections are conducted in marine transport to increase safety, security and quality performance. These inspections are conducted based on published CDI Ship Inspection Report.(CDI 2019)

For both chemical tankers and liquified gas carriers, it can be seen that two questions related with cyber security have been added to version 9.8.1 of CDI Ship Inspection Report that will enter into force on 02nd September 2019. CDI Ship Inspection Report has 14 sections. These sections are listed in the Table 3 below.

Section No	Topic
Section 1	Certification, Manning etc.
Section 2	Management and Personnel
Section 3	Bridge
Section 4	Mooring
Section 5	Cargo Operations
Section 6	Engine Department
Section 7	Operational Safety
Section 8	Health, Safety and Personnel Protection
Section 9	Firefighting
Section 10	Lifesaving
Section 11	Environmental Protection
Section 12	Security
Section 13	Hull and Superstructure
Section 14	Accommodation

Table 3: CDI Section List

Cybersecurity related questions are included under Section 12: Security. When these questions in the guideline are analysed, it is seen that "Recommended" category was designated for these questions. This means "Referenced to industry Codes of Practices". Additionally, these questions are included in the group "I". Group "I" means "Inspections questions' are for full inspection by the inspector".

In CDI SIR, it is shown 2nd version of GCSOS (The Guidelines on Cybersecurity Onboard Ships) as a reference created with the support of important marine authorities such as MSC-FAL.1/Cic.3, BIMCO, INTERTANKO and OCIMF. In fact, there is a striking point. Although GCSOS version 2 was referenced for criteria in SIR 9.8.1, 3rd version which is the latest version of GCSOS, was published at the end of 2018. Thus, an older version is referenced within CDI SIR.

Currently, how challenging is cybersecurity-related conditions in CDI inspections are unknown. Application of CDI SIR 9.8.1. version and observations noted by inspectors will give a general idea.

The cyber security related questions are shown below.

Question 12.11
The company provides guidance on cybersecurity

Author Comment
This criterion examines risk assessment. Additionally, preventive precautions for cyber threats and vulnerabilities are recommended. Also, contingency plan to be applied in case of cybersecurity is questioned.

Question 12.12

The crew has been trained in company guidelines, policies or procedures on cybersecurity.

Author Comment

It is expected from the crew to complete cyber security related training and to keep records of these training as evidence. Crew must be familiar with possible cyber threats and vulnerabilities.

2.2.4 RightShip

This firm provides vetting service for tankers and dry cargo vessels. In vetting inspections for tankers, SIRE questionnaires are used by RightShip. However, dry cargo vessels have their own questionnaire called "Inspection and Assessment Report for Dry Cargo Ships". This questionnaire for usage in inspection of dry cargo ships has 10 sections. The sections are shown the Table 4 below.

Section No	Topic
Section 1	Vessel Particulars
Section 2	Documentation
Section 3	Effectiveness of ISM System
Section 4	Safety, Security & Environmental Management
Section 5	Structural Condition
Section 6	Machinery Management
Section 7	Bridge Management
Section 8	Holds – Ventilation, Lighting Securing
Section 9	Condition o Cranes
Section 10	Inspection Summary

Table 4: Sections of RightShip's Questionnaire

Cybersecurity related questions are included under Section 4: Safety, Security & Environmental Management. These questions are listed below

Question 4.7.1

Does the vessel and/or company have documented software/firmware and hardware maintenance procedures?

Author Comment

Maintenance reports of IT/OT systems are desired to be examined. Additionally, existence of a procedure that needs to be applied prior to any software or firmware update is questioned.

Question 4.7.2

Does the vessel and/or company have any cyber security procedures?

Author Comment

This question examines conducting risk assessment against cyberattacks. Additionally, it is possible to control existence of response in case of a cyberattack.

Question 4.7.3

Does the vessel and/or company provide any cyber security training?

Author Comment

This question examines the awareness of crew regarding cyber security. The inspector would like to see training records as an evidence.

3 Conclusion

As a result of benchmarking meetings among tanker operators and interviews with key persons of tanker operators, it was observed that cyber security related questions are asked during SIRE and TMSA inspections which are developed by OCIMF.

Although inspectors during SIRE and TMSA inspections fail to ask in-depth cyber security related questions, inspectors would like to ensure the existence of ship specific cyber security plan, restrictions of USB and RJ-45, cyber awareness training for ship crew and keeping records of these trainings. It is noted that observations are written to ships with deficiencies at these points. Due to these observations, tanker operators are accelerating their precautions related to cyber security.

Since a new version of CDI as a non-profit organisation will include cyber security related questions as of 02nd September 2019, effects on tanker industry is not predicted yet.

RightShip places cyber security related questions in its questionnaire which are prepared for dry cargo vessels. This challenged dry cargo vessel operators. However, RightShip is a private company on contrary to non-profit CDI or OCIMF. Additionally, this company does not have "Consultative Status" such as OCIMF that is given by IMO. This decreased its effect on dry cargo vessel operating firms.

Currently, for all vessels other than tankers and dry cargo vessels, there are no implementation that force these types of vessels to take precautions against cyber threats. Shipping companies that operate other vessel types solely require to add maritime cyber security related necessities to their SMS manuals in compliance with ISM Code until 01st January 2021.

There are two intersection cases where SIRE, TMSA, CDI and RightShip vetting questionnaires coincide. These are cyber security risk assessment and providing cyber security related training to ship crew. Similarly, ISM Code will demand cyber security risk assessment from ship operators as of 01st January 2021.

References

Balduzzi M, Pasta A, Wilhoit K. 2014. A Security Evaluation of AIS Automated Identification System.

Bhatti J, Humphreys T. 2014. Covert control of surface vessels via counterfeit civil GPS signals

Blake T. 2017. Hackers took 'full control' of container ship's navigation systems for 10 hours . [accessed 2019 Aug 31]. https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-ihs-fairplay/

CDI. 2019. CDI Introduction . [accessed 2019 Aug 31]. https://www.cdi.org.uk/Introduction.aspx

Clarksons. 2018. Update on 2017 Data Breach . [accessed 2019 Aug 31]. https://www.clarksons.com/news/notice-of-cyber-security-incident-ckn/

CyberKeel. 2014. Maritime Cyber Risks.

Goward D. 2017. Mass GPS Spoofing Attack in Black Sea? . [accessed 2019 Aug 31]. https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea

Graham L. 2017. Shipping industry vulnerable to cyber attacks and GPS jamming . [accessed 2019 Aug 31]. https://www.cnbc.com/2017/02/01/shipping-industry-vulnerable-to-cyber-attacks-and-gps-jamming.html

Havold JI. 2010. Safety culture and safety management aboard tankers. 95:511–519.

Humphreys T. 2017. Ships fooled in GPS spoofing attack suggest Russian cyberweapon . [accessed 2019 Aug 31]. https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/

IMO Resolution MSC.428 (98).

ISM Code. 2014th ed.: IMO.

Karti EN. 2017. Vetting and TMSA: Role and Requirements in the Shipping Industry.

Lund MS, Hareide OS, Jøsok Ø. 2018. An Attack on an Integrated Navigation System. Necesse. 3:149–163.

Maersk. 2017. Maersk News Release . [accessed 2019 Aug 31]. http://investor.maersk.com/news-releases/news-release-details/cyber-attack-update

OCIMF. 2019. [accessed 2019 Aug 31]. https://www.ocimf.org/organisation/introduction.aspx

Shefi A. 2017. Tests Show Ease of Hacking ECDIS, Radar and Machinery . [accessed 2019 Aug 31]. https://www.maritime-executive.com/article/tests-show-ease-of-hacking-ecdis-radar-and-machinery

SIRE. 2019. [accessed 2019 Aug 31]. https://www.ocimf.org/sire/about-sire.aspx

Skou S. 2017. CEO: Cyber Attack to Cost Maersk Up to USD 300 Mn . [accessed 2019 Aug 31]. https://worldmaritimenews.com/archives/227337/ceo-cyber-attack-to-cost-maersk-up-to-usd-300-mn/

The Local. 2014. State-sponsored hackers spied on Denmark . [accessed 2019 Aug 31]. https://www.thelocal.dk/20140922/denmark-was-hacked-by-state-sponsored-spies

WMN. 2018. COSCO Shipping Lines Falls Victim to Cyber Attack . [accessed 2019 Aug 31]. https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/