Maritime Cyber: Threats and Challenges

CDR (ret.) Eyal Pinko

The world of shipping and maritime transportation *has experienced a major transformation in recent years, and with the growth in connectivity, communication, digitization, automation and integration of information systems and logistics systems of the sea-ports, vessels and the shipping companies.*

The technological transformation *of the vessels and the sea-ports is occurring simultaneously with major upward trends in the quantity of maritime cargo transportation and the increasing number of vessels and the size of them.*

This is as a result of globalization processes and the growth in global trade and the global economy, the increasing demand for energy, and the growth in economic activity in exclusive economic zones (EEZ) all over the world.

Cyber attackers view the seaports and the shipping companies as quality targets, because the amount of information they possess, the high turnover in the industry and the technological vulnerability of the systems. Cyber attackers see high value in attacking the maritime industry.

The goals of cyber-attacks on the maritime industry and on maritime assets and infra-structure might be financial profits, influence on public opinion, reputation damage, political gain or for military purposes, such as disrupt or shut down nation's critical assets as part of hybrid warfare strategy.

This paper will describe the threats and challenges on the maritime industry.

The Threat

In 2011, a cyber-attack was carried out against the port of Anvers[1]. The attackers were a drug cartel that penetrated the cargo management systems and changed bills of lading in order to conceal the smuggling of drugs. Attacks with similar objectives have been carried out in the port of Antwerp and against various authorities in Australia during the years between 2011 and 2013. In 2011, the Iranian national shipping company, IRISL, was attacked by unknown cyber-attackers[2]. During the cyber-attack, the company's entire database was erased, including information on cargo, ships and containers.

[1] Sea trade maritime news, Antwerp incident highlights maritime IT security, 21/10/2013, retrieved from: https://www.seatrade-maritime.com/news/europe/antwerp-incident-highlights-maritime-it-security-risk/

[2] Reynolds Hutchins, Carriers threatened by cyberattacks, experts warn, 3/3/2015, retrieved from: https://www.joc.com/maritime-news/container-lines/carriers-threatened-cyber-attacks-experts-warn_20150303.html

In October 2013, a cyber-attack was carried out against a cruise ship through the Automatic Identification System (AIS)[3]. As a result of this cyber-attack the identity and location of the ship were changed. The attack was carried out by an Italian academic as a demonstration only and as a warning signal.

During that year, there were also two cyber-attacks on two oil drilling rigs, one off the coast of Africa which caused it to tilt on its side and sink and the other against a South Korean rig that shut it down for 19 days[4].

In June 2017, a cyber-attack changed the cyber awareness at the maritime domain. This cyber-attack was carried out against MAERSK, the largest shipping company in the world. The attack continued for about a week and shut down tens of thousands of computer terminals in the company's branches worldwide and by that shut down services to customers and. The attack caused the company damage of more than $400 million[5].

Following the MAERSK attack, there were other attacks against ports and shipping companies all over the world.

In July 2019 the US coast guard publish[6] that a cyber-attack took place in February 2019 on a merchant vessel heading to the Port of New York. The attacked vessel could not keep on its sail to the port, and the crew reported that their shipboard network had been "totally debilitated" by malware. They couldn't resolve the issue, and neither could the shipping company's system administrators, working onshore.

The US coast guard sent a intimidate team onboard the vessel, that solves the problem and let the vessel sail to its destiny at the port of New York.

It is not the first time that a vessel was under a cyber-attack. During August 2017, A U.S. Navy guided-missile destroyer has collided with a merchant ship in waters east of Singapore and the Straits of Malacca. At first the US navy published that the incident accrued due to a cyber attack on the navigation systems of the ships, made the ship deviate from its course. But after a while the navy published that the collision caused by a human navigation error. Maritime cyber experts do believe that this incident caused by a cyber attack[7].

---

[3] San Simon and Duch, Weaknesses in ship tracking systems, 11/4/2014 retrieved from: http://www.lsansimon.com/en/weaknesses-in-ship-tracking-systems/

[4] Jeremy Wagstaff, All at sea: Global shipping fleet exposed to hacking threat, 24/4/2014, retrieved from: https://www.reuters.com/article/us-cybersecurity-shipping/all-at-sea-global-shipping-fleet-exposed-to-hacking-threat-idUSBREA3M20820140423

[5] Andy Greenberg, The untold story of NotPetya, the most devastating cyber attack in history, 22/8/2018, retrieved from: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[6] James Rundle, Coast guard details February cyber attack on ship, 26/7/2019, retrieved from: https://www.wsj.com/articles/coast-guard-details-february-cyberattack-on-ship-11564133401

[7] *Chris Demchak* et al., Navy Collisions: Competence, overload and cyber factors, 29/8/2018, retrieved from: https://www.maritime-executive.com/editorials/navy-collisions-competence-overload-and-cyber-factors

In most cases of cyber attacks, the attackers are not identified, even though the damage caused by them includes disruption or shutdown of services provided by ports and shipping companies and is manifested in economic damage, ecological damage, damage to reputation and even threats to security.

The world of shipping and maritime transportation has experienced a major transformation in recent years, and in particular with the growth in connectivity, communication, digitization, automation and integration of information systems and logistics systems of the sea-ports, Vessels and the shipping companies and their customers.

Ports operate numerous computerized systems for port management, loading and unloading of containers and cargo, movement and storage within the port, billing and customer's services systems, physical security systems, and maritime control systems (Vessel Traffic Management System – VTMS), etc.

All of the systems are connected by means of the Internet, satellite communication systems, and are also connected to the vessels.

Vessels are equipped with numerous systems: detection and navigation satellite systems (Global Navigation Satellite System – GNSS), identification and monitoring of ships (Automatic Tracking System – AIS[8]), loading of navigation maps (Electronic Chart Display and Information Systems – ECDIS), control of the engines and steering, control of various sensors (such as monitoring of fuel, oil, water flow, fire/smoke, etc.), control of cargo and transshipment, etc.

The various systems onboard a vessel are interconnected and integrated, as well as being connected to the port and the shipping companies by means of satellite communication and other channels of communication.

The technological transformation of the vessels, the shipping companies and the sea-ports is occurring simultaneously with major upward trends in the quantity of maritime cargo transportation and the increasing number of vessels and the size of them, as a result of globalization processes and the growth in global trade and the global economy, the increasing demand for energy, and the growth in economic activity in exclusive economic zones (EEZ) all over the world.

[8] Chris Lo, GPS spoofing: what is the risk for ship navigation, 15/4/2019, retrieved from: https://www.ship-technology.com/features/ship-navigation-risks/

The global economy processes are based primarily on maritime trade and transport and there are already today about 8300 seaports in more than 210 countries and more than 52,000 cargo ships. It is expected that by 2023 there will be about 68,000 such ships[9].

The annual rate of growth in the expected volume of maritime trade and transportation is expected to reach about 3.2 percent during the next five years and already today more than 80 percent of global trade by volume goes by the seas.

The global economic changes, the increased importance of the ports and shipping to the economies of the world, the integration of technological advances, the multiplicity of seaport and ship systems and the connectivity between them are increasingly exposing ports and ships to cyber threats.

With the growth of global economy and maritime transportation, there is still no world regulation concerning cybersecurity and the measures should be taken in order to prevent cyber attack on the maritime industry. In June 2017[10], the International Maritime Organization (IMO), which is the organization that sets rules for security and safety for the maritime industry, published short code of practice to the maritime industry. The IMO is working on cybersecurity regulation which are about to be published as a draft on the first quarter of 2020, and expected to be mandatory for every vessel from the first quarter of 2021.

Cyber attackers view the ports and the shipping companies as quality targets, in view of the huge amount of information they possess, the high turnover in the industry and the technological vulnerability of the systems.

Cyber attackers which are being operated and used by criminal organizations, terror organizations, activists or nation-states are searching for ways and methods to exploit technological advances and systems in order to carry out cyber-attacks on the seaports, on shipping companies and even on vessels.

The goals of cyber-attacks on the maritime industry and on maritime assets and national infrastructure might be financial profits, influence on public opinion, reputation damage, political gain or for military purposes, such as disrupt or shut down nation's critical assets and national infrastructure as part of hybrid warfare strategy, using cyber attacks in order to gain military or political purposes.

[9] UNCTAD, Merchant fleet, 2018, retrieved from:
https://stats.unctad.org/handbook/MaritimeTransport/MerchantFleet.html
[10] IMO, Maritime Cyber Risk, retrieved from:
http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/cyber-security.aspx

Cyber threats to seaports and shipping companies

Sea ports uses many and different systems in order to operate the sea side and shore side logistics.

The drawing below shows the main systems used by the ports:

Figure 1 -Port's main systems[11]

Following are the types of cyber-threat faced by seaports and shipping companies:

a. The partial or complete shutdown of a port for a long period of time, which will affect imports and exports to and from the country and the services provided by the port, as well as the country's chain of supply (such as the country's ability to provide for the energy and food supply needs of its citizens).

The shutdown of the port can be accomplished by several means, for example:

1. The shutdown/disruption of the port management system (TOS – Terminal Operation System).
2. The shutdown or disruption of the cranes and transportation systems (loading/unloading and storage of containers).

b. Economic damage caused by the disruption of port's information systems and the alteration of identity records of containers, including their location at the port's yard and their destination (the customer and his location).
c. Mass destruction caused by hazardous substances that are found in large quantities in the ports and on ships being loaded and unloaded.
d. The overturning of a ship in the port, which is liable to partially or completely close the port, by means of a change in the loading plans of containers in the TOS system and a

[11] https://homeport.uscg.mil/Lists/Content/Attachments/2203/OCIA_Consequences%20to%20Seaport%20Operations%20from%20Malicious%20Cyber%20Activity.pdf

change in a ship's center of gravity which will affect its stability in the water, especially at the open sea.

Undesirable intervention and a change in the loading plans within the TOS may even lead to the sinking of a ship at sea.

e. Inability to monitor the port's traffic in order to control entry and exit of ships by penetrating the VTMS systems which controls the seaborne activity in the port and in the sea routes to the port.
f. Physical penetration of terrorists or criminals into the port (from land or from sea) using manipulation or shutdown of the security systems, including sensors, cameras and command and control sites in the port.
g. Smuggling good by changing and manipulating the vessel's manifests, by penetrating the information systems of the ports or the shipping company.
h. Ecological damage by damaging the port's systems or ships' systems in the port.
i. Damage to the port's or the shipping company's public image and reputation.
j. Gathering of sensitive national and organizational information from the port's information systems.

A cyber-attack on a seaport or on shipping companies can be carried out by the cyber attackers by means of the Internet (for example be Denial of Service attacks, ransom attack, brute force attack, etc.), or by the disruption of satellite navigation systems, physical penetration or by attacking the organizational supply chain, and by attacking port's or shipping companies' suppliers can gain vital information or control on the port's systems.

Cyber threats to Vessels

Main systems that are being operated onboard ship can be divided into several groups:

1. Navigation and identification
2. Chief engineering – Engines and power
3. Information systems (IT) and management systems
4. Communication
5. Crew's personal systems

Those systems described in the next drawing:

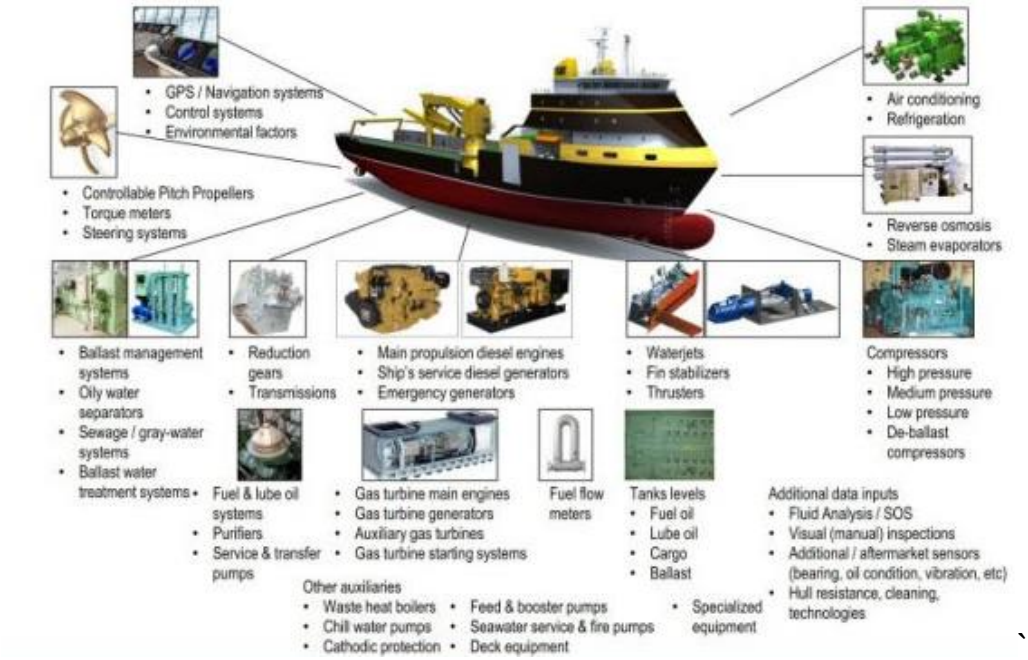

Figure 2 -Vessel's main systems[12]

The critical systems that might be exposed to cyber attacks onboard vessels are:

- **Communications systems**, from satellite connections to Wi-Fi networks to public address and alarm systems;
- **Bridge and navigation systems**, like GPS and other positioning and charting systems, The AIS system and the Global Maritime Distress and Safety System;
- **Propulsion and machinery power control systems**, like the engine governor and integrated ship controls;
- **Access control systems**, like the closed-circuit cameras, shipboard security alarms, and bridge navigation alarms;
- **Passenger information systems**, like financial and billing systems and electronic health records for those who visit the doctor;
- **Passenger-facing networks**, like public Wi-Fi and guest entertainment systems;

[12] https://siliconangle.com/2016/12/08/making-ships-run-time-predictive-analytics/

- **Core infrastructure systems**, like routers, switches, firewalls, intrusion prevention systems, and security event logging;
- **Administrative systems**, like crew tracking and personnel systems and crew-facing Wi-Fi or networks.

The risk of a cyber-attack on vessels (whether the vessel is in the port or at the open seas) are of the following types:

a. Overturning or sinking of a ship in the port or at sea, which can be achieved by penetrating the ship's loading planning program, changing the ship's loading program, and by that changing the center of mass of the ship. By overturning or sinking of a ship a cyber attacker can create a partial or complete closing and disruption of the port or a shipping lane.
b. Taking control remotely of a ship's steering and navigation systems which will enable the attacker to inflict the following types of damage:
    1. To navigate the ship to an undesirable route or cause a collision with another ship or some other object (a port, a pier, an oil drilling rig and the like).
    2. To paralyze a ship at sea by penetrating and overcome its navigation systems or ship's engines and power generators.
    3. To eliminate the ability to build a maritime picture for navigation at sea by attacking the radar systems, command and control or other computerized navigation means and systems such as the automatic updating map service (which is being downloaded from the internet by satellite communication for example).
    4. To hijack a ship for purposes of terror or piracy by taking control of its systems and stop it in the middle of the ocean[13].
c. To carry out a mass terror attack using hazardous materials that are to be found in large quantities on ships while they are loading/unloading or at sea.
d. To cause ecological damage through the release of fuel or other polluting substances.
e. Smuggling by means of altering or fabricating the ship's bills of lading (manifest).
f. Damage to public image or reputation that will cause economic losses to shipping companies.

A cyber-attack on a vessel can be accomplished through penetration by the vessel's communication channels (such as satellite, RF or AIS) to the vessel's control and navigation system, or by the disruption of the global navigation system (GNSS) or an attack on the chain of supply of the vessel.

[13] An interesting event if the February 2019 event in which a container vessel was stopped about 200 nm from the shore of New York, without being able to sail, after it suffered from massive cyber attack. The US coast guard sent a intimidate team onboard the vessel, that solves the problem and let the vessel sail to its destiny at the port of New York. Not many detailed revealed on that event. Five month later the US coast guard published the event and with it published recommendations and code of practice to ship's owners, in order to implement cyber security measures onboard ships.

Cyber attackers might attack a vessel using the AIS channel as a penetration point[14]. By using that the attack can achieve for example:

- Modify all ship details, including position, course, cargo, flag state, name, Mobile Maritime Service Identity (MMSI) status etc.
- Create fake vessels with identical details e.g. an Iranian vessel with nuclear cargo could appear off the US coast.
- Create and modify Aid to Navigations (AToN) entries, such as buoys and lighthouses. This leads to scenarios such as blocking the entrance to a harbour, causing a ship to wreck, etc.
- Create and modify marine search and rescue aircraft such as helicopters and light aircraft e.g. make a coast guard helicopter carry out a search and take off on a reconnaissance trip.
- Fake a 'man-in-the-water' distress beacon at any location that will also trigger alarms on all vessels within approximately 50 km.
- Fake a CPA alert (Closest Point of Approach) and trigger a collision warning alert. In some cases this can even cause software on the vessel to calculate an alternative course to avoid the collision, allowing an attacker to physically direct the vessel in a certain direction.
- Send false weather information to a vessel, e.g. to advise of storms approaching its course.
- Force all ships to send AIS traffic more frequently than normal, resulting in a flooding attack on all vessels and marine authorities in the area.

All this is possible because the AIS protocol was designed without taking into account, apparently, security considerations.

More than 400,000 ships are using the AIS tracking system, obligatory for all commercial (non-fishing) vessels over 300 metric tons, as well as all passenger ships, regardless of their size and tonnage.

From the GNSS systems (Global Navigation Satellite Systems), in the last years there a numerous report on GPS spoofing incidents at the Black Sea, by at least 20 ships[15]. GPS spoofing might cause ships to report their location at a wrong spot and by that to cause wrong navigation to their destiny.

Another damage can be caused by manipulating the GPS synchronized time (1 PPS), which can disrupt the integration with information systems at the shipping companies or at the ports via the satellite communication link.

[14] San Simon and Duch, Weaknesses in ship tracking systems, 11/4/2014 retrieved from: http://www.lsansimon.com/en/weaknesses-in-ship-tracking-systems/

[15] Michael Jones, Spoofing in the Black Sea: What really happened?, 11/10/2017, retrieved from: https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/

Challenges in providing cyber protection to ports and vessels

Protecting ports and shipping against cyber threats is a complex task. Following are some of the challenges:

1. Development of an organizational/security culture in the ports and in the shipping companies, which will ensure secure behavior and personal responsibility among the employees and the management levels, in addition to the assimilation of procedures, awareness and work methods for the improvement of organizational preparedness against cyber-attacks.
2. Shipping companies manage ports, goods and cargo in many countries, with a wide geographical dispersion. This makes it difficult to create a unified defense strategy that will provide protection to all of the ports and the connectivity between them.
3. There are many ports, shipping companies and ships operating worldwide without a unified configuration of information systems, detection and navigation systems, communication and control, etc.
4. There are various crews operating on the ships, with a variety of nationalities and very often with little security awareness and no control or supervision by an information security professional.
5. Supervision and monitoring of threats around the clock and throughout the year, including real-time monitoring and warning and the ability to deal with a threat within the shortest time possible.

Therefore, it is necessary to create cyber protection and security solutions that are on the one hand as generic and economically feasible as possible and on the other hand provide solutions for the heterogeneous configurations of the various systems on ships and in ports and against the large number and variety of threats.

Conclusion

In the world of globalization and world economy derives growth in maritime shipping and transportation. The maritime trade becomes crucial for countries' economy, energy, security and sovereignty.

Side by side to the growth of shipping, the vessels themselves and the seaports become more and more sophisticated, advanced and controlled by computerized and automated systems.

The computerized systems running the ports and the vessels are connected by satellite communication and other means of communication, thus seaports, vessels and shipping companied live in one big eco-systems.

While the growth of maritime trade and technology within the maritime shipping, cyber attackers are targeting the maritime industry to gain financial profits, influence on public opinion, reputation damage, political gain or for military purposes.

Maritime cyber attackers, at the new age of piracy, can be crime organization (or lone criminals), terror organization, armature attackers and even nation states, willing to collect information on their adversary's infrastructure or to gain access and control on their systems as part of "under the radar" military acts.

Most of the maritime industry companies (from seaports to ship owners and shipping companies) are not ready and protected enough against cyber-attacks. Furthermore, there are no world regulation for the maritime industry yet, although the IMO (International Maritime Organization) is working on regulation that will fit the maritime industry, focusing on vessels. The IMO regulation is expecting to be published during 2021, and it will take years in order to implement the upcoming regulations.

The challenges of implementing cyber security measures, procedures and infrastructure in the maritime industry companies are complicated, yet they should be in order to be more prepared, secure and resilient for cyber attack crisis.