MARITIME CYBER THREATS AND CHALLENGES

CDR (ret.) Eyal Pinko*, PhD Candidate,
Bar Ilan University

Abstract

The maritime trade becomes crucial for countries' economy, security and sovereignty. Side by side to the growth of shipping, the vessels themselves and the sea-ports become more and more sophisticated, advanced and controlled by computerized and automated systems.

Most of the maritime industry companies (from sea ports to 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,

* **Eyal Pinko** (Navy Commander, retired) served in the Israeli navy for 23 years. In those years he served 4 years in operational duties, 12 years as a project manager for several development programs, and for more than 6 years, as the head of operational and research branch at the Israeli naval intelligence. He served for 5 more years as the head of division at the ministry of defense (Civilian rank equal to RADM). Eyal holds the Israel's security award, prime minister's decoration of excellence, DDR&D decoration of excellence, and IDF commander in chief decoration of excellence. Since August 2017, he is a senior consultant for cyber and maritime cyber, focusing in cyber strategy, risk assessment, threat analysis, risk management and awareness. He holds bachelor's degree with honor in electronics engineering, and two master's degrees with honor in political science and in organizational development. Since 2015, he has been a PhD candidate at the Bar-Ilan university and a Research Fellow at the Haifa Maritime Policy and Strategy Research Center. His research focuses on strategy, asymmetrical and hybrid warfare, cyber and weapon systems.

focusing on vessels. The IMO regulation is expecting to be implemented during 2021.

Keywords: Maritime industry, cyber threats, cyber protection, seaports, vessels.

The Threat

In 2011, a cyber-attack was carried out against the port of Anvers. 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. During the cyber-attack, the company's entire database was erased, including information on cargo, ships and containers.

In October 2013, a cyber-attack was carried out against a cruise ship through the Automatic Identification System (AIS). 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.

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.

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

In most cases, 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 the 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), 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.

The global economy processes are based primarily on maritime trade and transport and there are already today about 8700 sea-ports 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.

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.

The 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 sea-ports, on shipping companies and even on vessels.

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.

Cyber threats to sea-ports and shipping companies

Following are the types of cyber-threat faced by sea-ports 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/disruption of the cranes and transportation systems (loading/unloading and storage of containers).

b. Economic damage caused by the disruption of information systems and the alteration of identity records of containers, including their location and destination.

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 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.

f. Physical penetration of terrorists or criminals into the port (from land or from sea).

g. Smuggling good by changing the vessel's manifests.

h. Ecological damage.

i. Damage to the port's or the shipping company's public image and reputation.

j. Gathering of sensitive national information.

A cyber-attack on a sea-port or on shipping companies can be carried out by means of the Internet, the disruption of satellite navigation systems, physical penetration or attacking the organizational supply chain.

Cyber threats to Vessels

The risk of a cyber-attack on vessels (whether 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.

    3. To eliminate the ability to build a maritime picture for navigation at sea.

    4. To hijack a ship for purposes of terror or piracy.

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.

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. Therefore, it is necessary to create cyber protection 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 against the large number and variety of threats.

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.

Conclusion

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

Side by side to the growth of shipping, the vessels themselves and the sea-ports 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 sea ports, vessels and shipping companied live in one big eco-systems.

While the growth of sea 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.

Most of the maritime industry companies (from sea ports to 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 implemented during 2021.

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.