אוניברסיטת חיפה
University of Haifa
جامعة حيفا

HMS
מרכז חיפה למחקרי מדיניות ואסטרטגיה ימית
Haifa Research Center for Maritime Policy & Strategy

MARITIME STRATEGIC EVALUATION FOR ISRAEL 2017/18

Chief editor: **Prof. Shaul Chorev**

Edited and produced by: **Ehud Gonen**

Maritime Cyber Warfare – Developments in the Past Year

Eitan Yehuda

During the last two years, there have been a number of noticeable trends that have changed the approach of governments and military organizations, as well as private companies, to the world of maritime cyber. However, this awareness has apparently not yet reached a level that will lead to concrete systemic steps to counter the threats. This is in contrast to what is happening, for example, in the financial and defense realms:

1. There are a large number of attacks and disruptions of systems on both military and civilian ships and also on mega-yachts.
2. The rapid development of Internet of Things technology (IoT),[1] partly as a result of a number of attacks on sensors (which constitute the IoT network) and the adaption of defensive solutions to the maritime world.
3. Global technological development of autonomous vessels and the understanding that the capture of such a vessel is a serious threat since there is no crew on board in order to react to an attack.

The article published by the Corporate & Specialty Allianz Group (AGSC),[2] which describes the main risks in the shipping world and analyzes the main cases of financial losses in 2017 in the shipping domain, reports that cyber attacks on ships and in particular on ports are on an upward trend and that thought and effort need to be invested to counter this threat.

Examples of cyber attacks in the maritime domain in 2017

1. A type of malware called "Zombie Zero" was introduced into the scanners used in maritime shipping, which are used to check the content of packages and cargo for security purposes and the detection of explosives. The malware, which apparently was introduced by Chinese hackers, makes it possible to remotely take control of the computer systems of ports where the scanners are installed. The malware exploits a known weakness in the outdated Microsoft XP operating system. By way

1 The Internet of Things (IoT) is a network between objects or "things that enables advanced communication between the objects and the ability to gather and exchange information. The IoT includes among other things the “smart house” and the “smart city”, smart cars, smart management of the electricity grid, wearable accessories (such as watches and shoes), monitoring of instruments (heart implants, security systems, etc.) and more, and can relate to a wide variety of appliances both inside and outside the home. The development of the IoT in coming years is expected to facilitate automation in many walks of life. At this stage, the IoT market is only in its infancy; however, according to the Gertner research company, by the end of 2020, the number of instruments that are connected to the Internet worldwide will reach about 26 billion. According to the McKinsey consulting company, ‘the global market for IoT is expected to grow to $620 billion by 2025.’" (Know2 magazine, March 2016).

2 Safety and Shipping Review 2016 by Allianz Global Corporate & Specialty (AGCS) available at www.agcs.allianz.com, page 34.

of this scanner, the Chinese hackers remotely took control of the communication and information systems of the shipping companies. It is worth mentioning by the way that the development of the malware was financed by the Chinese government, which was revealed by the TRAPX cyber company.

2. South Korea reported that hundreds of its vessels were forced to return to port due to the remote takeover by North Korean hackers of their GPS systems.
3. On June 17th 2017, a commercial ship called the ACX Crystal collided with the USS Fitzgerald. Eleven minutes before the collision, malware called "WannaCry" attacked Maersk, one of the largest shipping companies in the world. Another commercial ship, the Evora, which belongs to Maersk and which was in radio contact with the ACX Crystal at that time was in the area of the collision (see the appendix for a map showing the collision and the location of the Evora). Seven crew members of the Fitzgerald were killed and in the official report published by the US Navy, it was claimed that there is no connection to any cyber attack and that the reason for the collision was human error.
4. Twenty commercial ships that belong to American companies reported that their GPS systems were disrupted while in the Black Sea.
5. In July 2017, Apple and Google released a security update against the malware "BroadPwn" which enables remote takeover of communication components installed on the systems of ships.
6. In August 2017, a commercial ship called the Alnic MC collided with the USS John S. McCain. As a result, 17 American sailors were killed and also in this case the investigation concluded that the reason for the collision was human error rather than a cyber attack.
7. An article published in *The Guardian* on November 11th 2017 reported that Clarksons, one of the largest shipping companies in the world, was attacked by ransomware which encoded its database. The company refused to pay the ransom demanded and requested that the authorities deal with the attack.

The events described above were published in much of the media, a fact that increased the exposure to the subject of cyber security in the realm of ports and shipping and to a deeper understanding, primarily among governments, that the threat is real and can cause economic damage and even loss of life.

The exposure has led venture capital funds and hi-tech companies that are involved in information security to devote thought to the subject and to develop protective measures also in the maritime domain. The common approach is currently to adopt protective technologies that are developed for IoT sensors for all of those systems in which there are sensors that control the main components of the ships (see the appendix for a list of the main systems in a ship in which sensors are installed).

According to this approach, the solution is provided starting from the level of the sensor (for example, an antenna that receives GPS signals), encoding of the communication range, upgrade of the operating systems and hardware and up to the level of the application.

Conclusion

The large number of cyber events in the maritime realm in 2017 led to a change in awareness of the threat. This can be seen in the allocation of funds by venture capital funds and the creation of a number of startup companies that are developing protective measures.

The development of IoT technology and the creation of business solutions that are based on this technology will be accompanied by development of the protection of these systems and in the future it will be possible to more easily adopt these solutions also in the maritime realm.

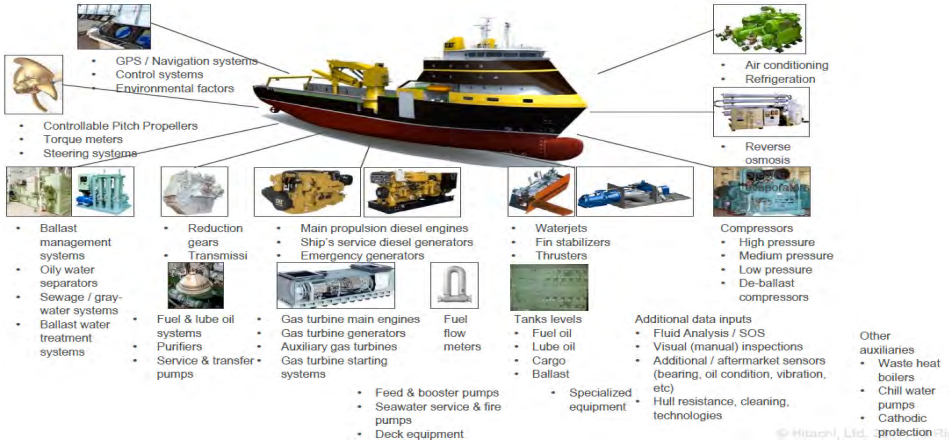

Figure 1 – List of main ship components equipped with sensors

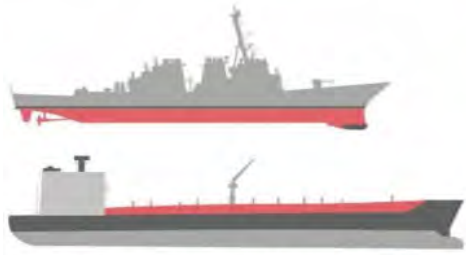

Figure 1 – Relative size of USS JOHN S MCCAIN

Figure 2 – Illustration Map of Approximate Collision Location

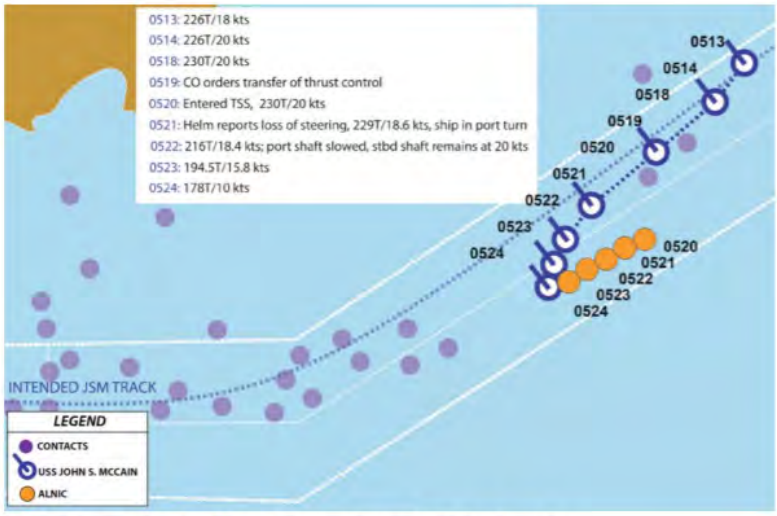

Figure 3 – Illustration Map of Approximate Collision Location

Figure 2 – The collision of the commercial ship Alnic MC with the USS John S. McCain[3]

3 DEPARTMENT OF THE NAVY OFFICE OF THE CHIEF OF NAVAL OPERATIONS 2000 NAVY PENTAGON WASHINGTON, DC 20350-2000.

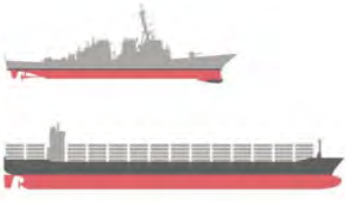

Figure 1 – Relative size of the USS Fitzgerald

Figure 2 – Illustration Map of Approximate Collision Location

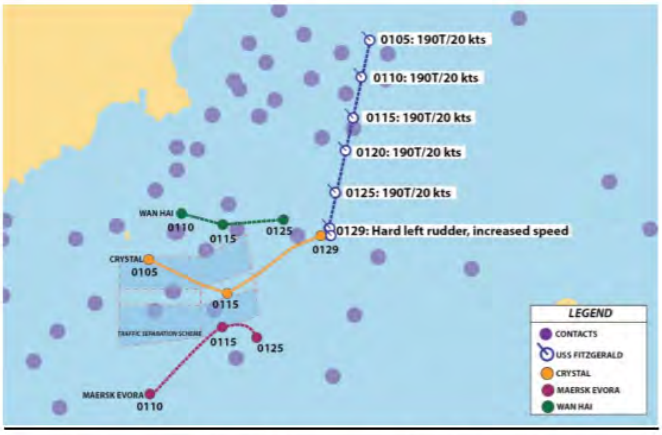

Figure 3 – Illustration Map of Approximate Collision Location