MARITIME STRATEGIC EVALUATION FOR ISRAEL 2022/23

Chief Editor: **Prof. Shaul Chorev**

Editor: **Dr. Ziv Rubinovitz**

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

HMS
המרכז לחקר מדיניות ואסטרטגיה ימית
Maritime Policy & Strategy Research Center

Cyber Threats to Maritime Platforms and Insights from Coping with the Covid-19 Pandemic

Itai Sela

Introduction

The process of reducing Europe's dependency on Russian energy supply, as a result of the war between Russia and Ukraine, and the recent gas discoveries off the coast of Israel, have put maritime platforms based on operational technology (OT) systems on the public agenda in Israel and around the world, marking them as a high-quality target for cyberattacks with widespread strategic, security, economic, environmental and state-related implications.

Since the outbreak of the Covid-19 pandemic, the use of the cyber-weapon on operational technology systems have expanded, for example, Microsoft has reported more than 200 cyberattacks, with more than 40% of them targeting operational networks and critical infrastructure.[1] A 2021 summary FBI report additionally indicates approximately 649 ransom attacks, causing damage to organizations related to critical infrastructure in the United States;[2] the discovery of the Incontroller/Pipedream malware which was designed to damage OT systems and has a rare and particularly dangerous attack capability (it is estimated to be a state-sponsored software development);[3] an attack using the "Ekans"ransomware that targeted OT systems;[4] a cyberattack – against commercial satellite communication networks (SATCOM Network);[5] a widespread cyberattack that damaged OT systems at oil terminals in Western Europe (the Netherlands, Belgium and

1 Ravie Lakshmanan ,Microsoft Documents Over 200 Cyberattacks by Russia Against Ukraine, *The hacker news* ,April 29, 2022.

2 Federal Bureau of Investigation, Internet crime report 2021, FBI IC3, 2022.

3 Nathan Brubaker, Keith Lunden, Ken Proska, Muhammad Umair, Daniel Kapellmann Zafra, Corey Hildebrandt, Rob Caldwell, Incontroller: New State-Sponsored Cyber-attackTools Target Multiple Industrial Control Systems, *Mandiant*, April 13, 2022; Pipedream: Chernovite's Emerging Malware Targeting Industrial Control Systems, *Dragos*, Free whitepaper, April 2022.

4 Scott Ferguson, New Ransomware Targets Industrial Controls: Report, *Info risk today* February 5, 2020.

5 Antony J. Blinken ,Attribution of Russia's Malicious Cyber Activity Against Ukraine, U.S. Department of State, May 10, 2022.

Germany);[6] an attack on a drilling company that operates offshore drilling rigs;[7] and an attack on a manufacturer of maritime OT systems.[8]

This article analyzes the cyber threats to civilian maritime platforms while addressing the unique cyber-related characteristics and vulnerability of OT systems, located on maritime platforms. This article attempts to answer obvious questions which arise in this context: Is this a significant threat? And if so, is it possible to implement the strategies of coping with the Covid-19 pandemic when addressing maritime cyber threats?

Background

Over the past four decades, there has been considerable progress regarding the technologies used on maritime platforms (commercial vessels, passenger ships, drilling rigs, production platforms, etc.) – from platforms built in the early 1980s, and based on relatively simple technology, through platforms built at the beginning of the 21st century with increasing use of computer-based technologies and up to the platforms built in the last decade, which are almost entirely based on advanced computer technologies, both in terms of Information Technology (IT), and in terms of operational technology (OT).

The IT supports the control and transfer of information between maritime platforms and the company headquarters, various suppliers, seaports and different authorities with which the maritime platforms are in continuous contact. This technology uses satellite, cellular and wireless communication networks in order to transfer information between the maritime platform and the various parties onshore and offshore. The information network computers are usually located on the bridge, in offices and in the various sections and residences on the platform – these systems and networks are separated, by definition, from the OT systems and networks.

The OT serves as the interface connecting humans and machines, thus helping to perform critical operations. On average, there are about 70 operational systems on a maritime platform. These systems are provided and maintained by a variety of manufacturers, run on different types of operating systems (Win XP/7/10, Linux), run diverse applications, require a high level of reliability and availability, and are required to operate continuously 24/7, for most of the year. These systems are operated by maritime crew members who are required to work the platform in shifts around the clock for long periods of time (several weeks to several months, consecutively), and often without appropriate cyber defense training.

---

6 The Editorial Team, Cyber-attacks hit European oil terminals, *Safety4Sea*, February 4, 2022.

7 KCA Deutag Alpha Limited, Annual Report and Financial Statements for the year ended 31 December 2021, May 12, 2022.

8 Sam Chambers, Voyager Worldwide hit by cyber attack, *Splash247*, December 9, 2022.

Figure 1 illustrates different types of OT systems installed on maritime platforms, such as the Electronic Chart Display and Information System (ECDIS), which replaces paper navigation charts, optimizes navigation and prevents accidents by locating and presenting geographic information based on digital navigation charts and integration with additional sources of information (objects discovered by RADAR, GPS location, AIS data, depths, etc.); a RADAR (Radio Detection And Ranging) system which allows to create an image of navigational obstacles, assisted by electromagnetic radio waves, the BAMS (Bridge Alert Management System) located on the vessel's bridge helping on-duty officers manage the alerts received from the various systems; MCS (Machinery Control System), used to control, survey and monitor machinery systems such as engines, pumps, stability systems, and dedicated systems such as MPD (Managed Pressure Drilling) pressure control systems; BOP (Blowout Preventer) emergency disconnect systems; the VDR (Voyage Data Recorder) system that serves as the maritime "black box"connected to most of the navigation, machinery and safety systems on board the vessel; Dynamic Positioning (DP) systems, air conditioning, elevators, and various sensors such as GPS (Global Positioning System) and AIS (Automatic Identification System) that feed the various operating systems. The communication between the various systems on the platform is based on a 0183/2000 NMEA (National Marine Electronics Association) communication standard which is used in the maritime industry, and defines standards for electrical signals, protocols, data transfer time and specific formats.[9]

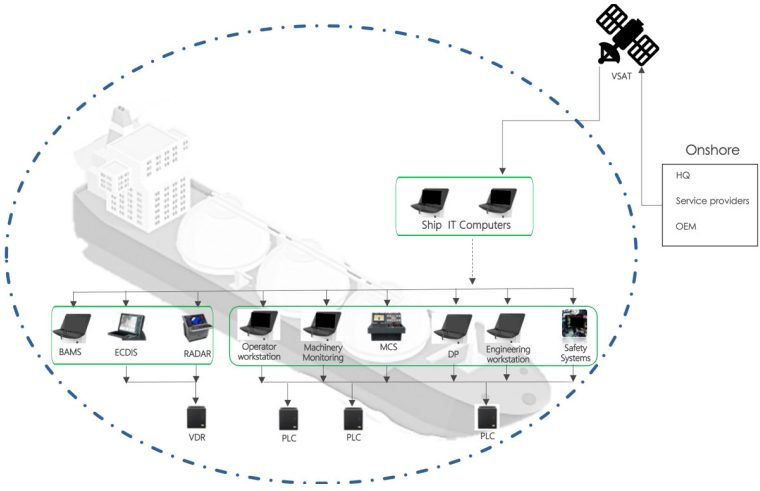

Figure 1: The layout of main OT systems in a commercial vessel

9 National Marine Electronics Association, NMEA 2000, standard for serial-data networking of marine electronic devices, Version 2, December 2014; Eric S. Raymond, NMEA Revealed, Retrieved December 2022.

The Unique Aspects of Operational Technology Systems from a Cyber Perspective

Over the past few years, a considerable increase in the use of the cyber weapon against maritime platforms and infrastructure has been observed.[10] The appearance of the cyber weapon, defined by Rid & McBurney as malicious software (malware), used to achieve military or intelligence goals as part of a cyberattack,[11] has made OT systems on maritime platforms extremely exposed and vulnerable to attacks, due to several factors that differentiate them and their environment.

The first factor is the fact that OT systems are based on obsolete operating systems (OS), which are not supported by the manufacturers, in terms of security and software updates. One of the main reasons for this is the distinct difference in the life expectancy of the maritime platform, which ranges from 20 to 30 years to the life expectancy of the various operating systems, which ranges from 10 to 20 years, and the life expectancy of the operating systems in OT systems, which ranges from 5 to 10 years. As a result, on most of the maritime platforms active today, the vast majority of the OT systems are based on obsolete operating systems that were developed in an era when awareness to cyber threats was not as advanced, and for this reason contain many inherent cybersecurity vulnerabilities. In addition, these systems are not supported by the manufacturer of the operating systems, for example, Microsoft's "Windows XP" operating system's technical support and security updates ended in April 2014[12] and the "Windows 7" operating system's technical support and security updates ended in January 2020.[13] Recently, the manufacturers of these operating systems began to market new systems based on "Windows 10", which is considered up-to-date and is still supported by Microsoft, but Microsoft has already announced that it will only support this software until October 2025.[14]

The second factor is the implications of the upgrade (cost and "standing time"). Although the manufacturers of the OT systems (on average about ten different manufacturers for one maritime platform) prefer and encourage the platform owners to perform a version upgrade every 4 to 6 years, the platform owners do everything in their power to avoid

---

10 F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, & M. Michaloliakos, Cybersecurity Challenges in the Maritime Sector. *Network*, 2, no. 1 (2022): 123–138.

11 Thomas Rid & Peter McBurney, Cyber-Weapons, *The RUSI Journal*, 157, no. 1 (2012): 6–13.

12 Eve Blakemore, Support for Windows XP ends in April 2014, *Microsoft*, April 30, 2013.

13 Windows 7 support ended on January 14, 2020, *Microsoft*, 2020.

14 Windows 10 Home and Pro, *Microsoft*, 2021.

these required upgrades and try to maintain and preserve the existing systems. This is because an upgrade of this scope can add direct costs of up to hundreds of thousands of dollars (on a commercial vessel) and up to tens of millions of dollars (on a maritime energy platform) to upgrade the systems themselves, in addition to the implications and costs involved in preparing the platform (stopping activity) for the purpose of the required upgrade. In view of today's market trends, according to which most maritime platforms operate using a "hot platform" method, which means continuous work with the exception of short breaks required for switching over from one contract to another, the prevailing trend in the industry is to only enter into short term contracts. Thus, any stoppage and attempt to implement any kind of system upgrade, which requires stopping activity for a period of two months to a year, will directly and significantly affect the profitability of the maritime platform.

The third factor is related to the segmentation of IT and OT communication networks. The communication networks deployed on a maritime platform can be divided into two kinds: IT networks that connect the various information systems and OT networks that connect the various OT systems. The common perception today in the maritime industry refers to the OT systems and networks as segmented and disconnected from the IT network and the Internet, for this reason, these networks are considered to be less exposed to various cyber threats. This, despite the fact that the accepted work practices in the maritime industry expose the networks and OT systems to the IT networks, creating a situation called a "flat network", which allows malware penetrating one network to spread relatively easily to other networks as well as to many critical OT systems on the platform.

The fourth factor is the attack vectors that the attackers use to penetrate and damage OT systems onboard maritime platforms. The first vector, as illustrated in Figure 2, is the External Attack Vector, which uses the platform's IT network (which is based on satellite, cellular and wireless communication media) and the many service providers (the company's headquarters, the company that leases the platform, regulatory national and international organizations, technical factors, maintenance, and supply) as a gateway to the OT systems on the maritime platform. After the malware has managed to enter one system on the platform, it will take advantage of the gaps in the segmentation of the networks and will spread relatively easily between the different networks and OT systems. One attack that used this attack vector was reported in February 2017 after a breach was detected in the OT system on a container ship sailing from Cyprus to Djibouti. According to reports, the attack file penetrated the vessel's IT network, gained access to the OT network, took over the vessel's navigation system for about ten hours, and in the process breached the vessel's safety and the crew's ability to operate the systems. According to the incident report, the attackers' intention was to gain full control of the

navigation systems and direct the vessel to an area where they could physically take control of it. Only after assistance from the company's headquarters was the crew able to regain control of the navigational system.[15]

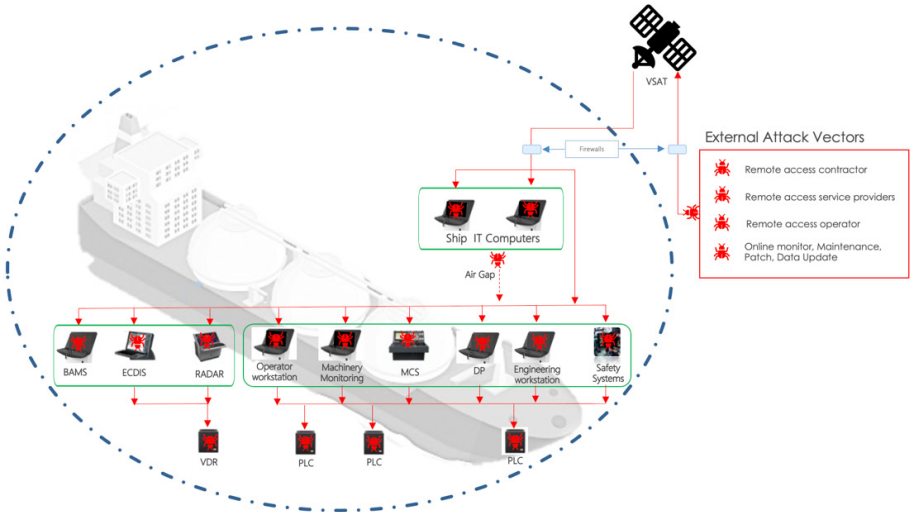

Figure 2: External attack vectors on vessels, and a description of the spread of malware from the IT systems to various OT systems

The second vector, as illustrated in Figure 3, is the Internal Attack Vector, which uses actors with routine activity access privileges to the OT systems (crew members and manufacturers' technicians working onboard), to unintentionally insert the malware from an IT computer into an OT system. Examples of attacks that used this attack vector are: a) In 2013, a cyberattack that succeeded in introducing malware into a shore technician's computer was reported. As part of routine maintenance on a maritime energy platform, unintentionally and unknowingly this technician transferred the malware from his computer to OT systems onboard the rig – an event that led to the shutdown of the rig after it became clear that the navigation systems, propulsion, dynamic positioning (DP) control and drilling systems were significantly damaged.[16] b) In 2018, it was reported that dormant malware was discovered in vessel systems after approximately 875 days. The incident report found that unknowingly and unintentionally, the service provider introduced the malware into the vessel's system using a portable memory drive (USB)

15 IMO, International Maritime Organization maritime knowledge centre "sharing maritime knowledge", *Current Awareness Bulletin*, XXIX(11), November 2017.

16 Zain Shauk, "Malware on Oil Rig Computers Raises Security Fears", *Houston Chronicle Energy*, February 23, 2013.

during a software update.[17] c) That same year, a technical malfunction was reported in two ECDIS systems on a new cargo ship. These were later discovered to be infected with malware which caused the delay of the ship's sailing, and hundreds of thousands of dollars' worth of damage.[18]

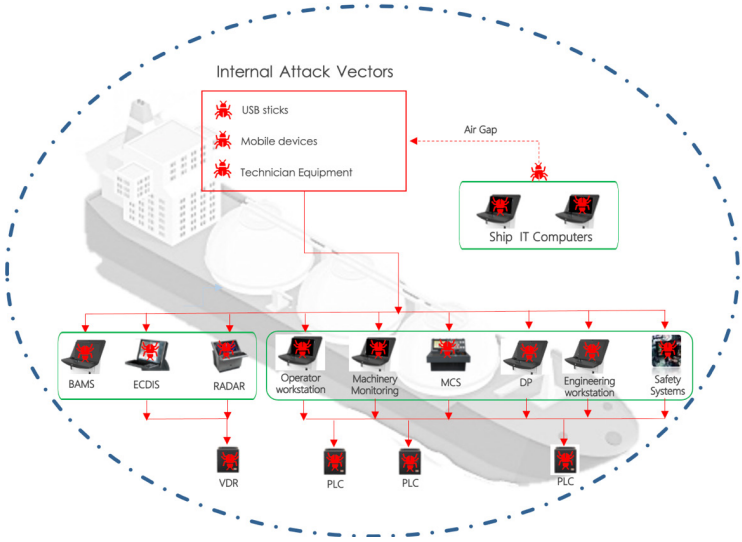

Figure 3: Internal attack vectors in vessels and the spread of malware to all OT systems

Is the Cyber Threat to Maritime Platforms Significant?

In order to address this question and in addition to collecting published data on cyber-attacks, key findings of several cyber-attack simulations were examined and analyzed here: the first simulation examined the feasibility and significance of a cyber-attack on critical OT systems on board vessels such as RADAR, ECDIS, and MCS.[19]

The second simulation examined the feasibility and significance of a cyberattack on a dynamic positioning system (DP) in an environment simulating a drilling rig.[20]

---

17 The guidelines on cyber security onboard ships, Version 4 (2021).

18 Ibid.

19 Northern California area maritime security committee, *cyber security Newsletter*, Edition 2018-07, July 2018.

20 Paola Rossi, Itai Sela, Adam Rizika, Diogenes Angelidis, Mark Duck, and Ron Morrison, Cyberdefence of Offshore Deepwater Drilling Rigs. *Offshore Technology Conference*, Virtual and Houston, Texas, August 2021.

As part of the feasibility of a cyber-attack on a radar system on a naval platform, malware was introduced into the RADAR (OT system), which is used as a navigational safety tool for the purpose of locating and warning of navigational obstacles and preventing collisions. The RADAR system transmits electromagnetic radio waves and displays the returning signals from the navigational obstacles on the RADAR display as a bright spot. The malware introduced into the RADAR system was able to create a manipulation, so that in the RADAR image shown to the navigation officer on the bridge, as can be seen in Figure 4, the navigational obstacles in the vicinity of the maritime platform did not appear (were concealed), and the alerts, which allow the navigation officer to understand that something is wrong, were not displayed.[21]

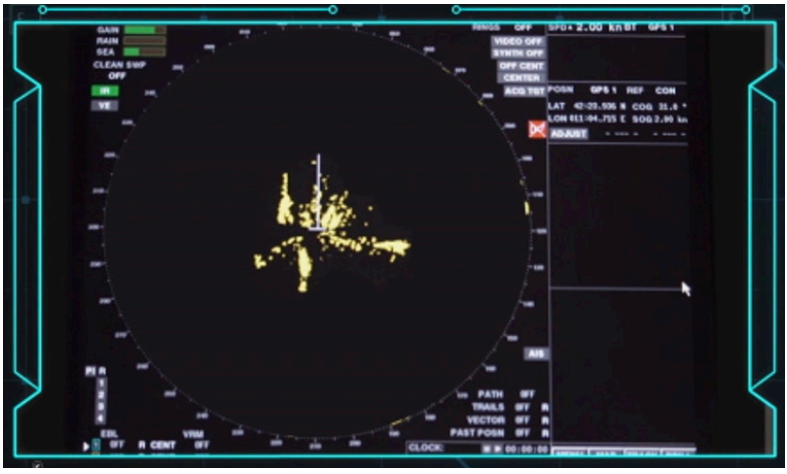

Figure 4: The RADAR display presented to the navigation officer on the bridge

This occurred despite the fact that in practice there were many navigational obstacles in the vicinity of the maritime platform, including those located further along the sailing route, that were concealed by the malware, as can be seen in Figure 5, in the real RADAR image (without the attack manipulation – marked with red circles).[22]

This simulation demonstrates that a cyberattack is capable of manipulating the data presented to the navigation officer and can lead to creating a false image of navigational obstacles, which can end in collision, loss of human life, environmental damage and damage to property.

---

21 Tests Show Ease of Hacking ECDIS, Radar and Machinery, *The Maritime Executive*, December 21, 2017.

22 Ibid.

Figure 5: The actual RADAR display that shows the obstacles that were concealed from the navigation officer using manipulation

Figure 6 shows a demonstration of a manipulation attack on a vessel's navigation system (ECDIS), which assists the navigation officer in creating a global plan and sailing route.[23] The left image of this figure shows the system display in which the position of the vessel in accordance to the navigational obstacles and the depth appear to be correct. Yet, as can be seen in the right image, the position of the vessel is different, and very close to the navigational obstacles. It is also apparent that the water depth is shallow and dangerous. This attack aims to present false information to the navigation officer, leading to incorrect decision making regarding the planning and safety of the voyage, to a deviation from the planned route and even to collision.

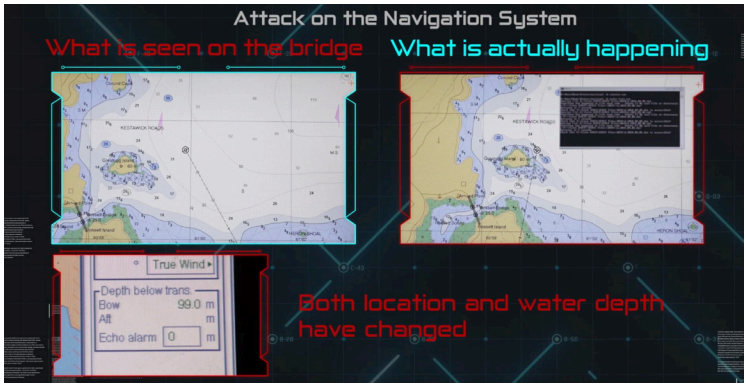

Figure 6: A Manipulation attack on the navigation system (ECDIS)

23 Ethical hackers demonstrate weaknesses in shipboard systems, *Digital Ship*, January 2, 2018.

Figure 7 shows a demonstration of a manipulation attack on a machine control system (MCS) that controls the vessel's engines, stability systems, balance and other systems that allow the machinery officer to activate and monitor the operation of the vessel's systems.[24] As can be seen from the data on this attack, the left image of the figure shows the machinery control display indicating one running pump, although in practice, as can be seen in the right image, this pump is not working at all, while several other pumps that are shown as turned off – are working without the machinery officer's knowledge. This attack's purpose is to prevent and disrupt critical operations and present false information to the machinery officer, thereby leading to unwanted and uncontrolled emission of liquids and gases, damage to the vessels' control, propulsion and steering systems, which can lead to financial and environmental damage, as well as to the loss of human life.

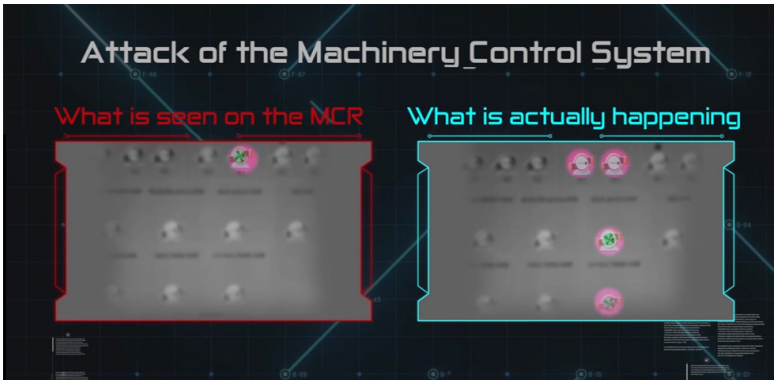

Figure 7: A Manipulation Attack on the Machinery Control System (MCS)

Simulation of a Cyber-Attack on a Dynamic Positioning System in a Drilling Rig Simulator

As part of the feasibility of a cyber-attack on a dynamic positioning system (DP) (OT system), the use of an internal attack vector was demonstrated. In this case, a laptop used by the manufacturer's technician was infected, without his knowledge, with malware. The malware took over the DP systems and spread to other critical and safety systems onboard the rig.[25]

---

24 The Challenge, *NavalDome Website*, Retrieved December 2022.

25 Rossi et al., Cyberdefence of Offshore Deepwater, 2021.

This demonstrates the ability of a malware to penetrate the cybersecurity measures currently in use on drilling rigs, gain full control over critical OT systems,[26] and even recreate, through a cyber-attack, similar malfunctions to those that led to the "Deepwater Horizon" oil spill in 2010 in the Gulf of Mexico, where 11 crew members loss their lives and which caused economic damage of more than $140 billion and extreme environmental damage, as can be seen in Figure 8.[27]

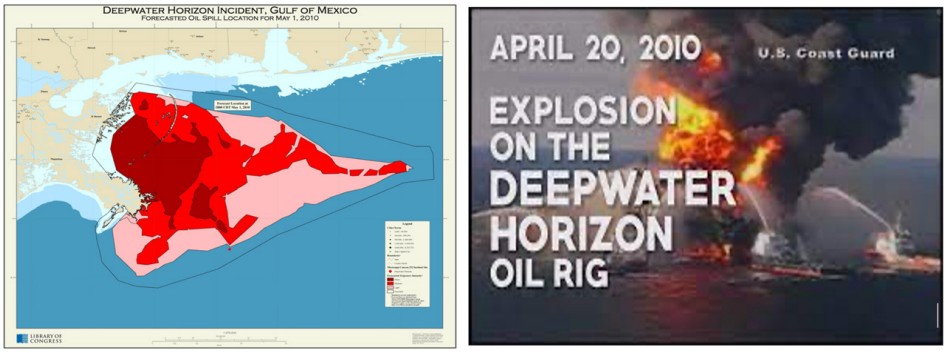

Figure 8: The 2010 "Deepwater Horizon" oil spill in the Gulf of Mexico

From the analysis of the cyber-attacks and the simulations on OT systems on different maritime platforms, it may be concluded that the cyber threat to maritime platforms is significant and has the potential to cause significant strategic damage with consequences related to the environmental, economic, geopolitical aspects and for human life.

Coping with These Threats, and Can Approaches Used for Coping with the Covid-19 Pandemic be Implemented for Cyber Defense?

After defining cyber threats to maritime platforms as significant, the following step was examining if it is possible to implement the coping approaches with the Covid-19 pandemic to defense approaches for maritime cyber threats. In order to answer this question, different defense approaches were examined, as well as their comparison with approaches for coping with the pandemic.

There are currently three main defense approaches in use for protecting civilian maritime platforms against cyber threats on OT systems. The first and most common approach

---

26 Mahesh Sonawane, Ryan Koska, Mike Campbell Riser failure study IDs well control weak links, *Drilling Contractor News,* March 15, 2012.

27 National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling. Report to the President, January 2011.

sees the human factor as mainly responsible for protecting the platform from cyber threats, and therefore focuses on cyber hygiene education and training of the crew members and technicians. This approach is similar to the one used to cope with the Covid-19 pandemic, which initially focused on education and training of the population (mandatory mask-wearing, social distancing and hand washing) and later was revealed to encounter difficulty dealing with complex threats such as cyber threats and pandemics. The second approach is based on the attempt to create a physical separation of networks, in order to mitigate and control the attacks. This approach is similar to lockdowns during Covid, and the implementation of technological monitoring solutions to identify and warn of abnormal or unauthorized activity following the penetration of malware is similar to the monitoring of cell phones, the positioning of roadblocks and the existence of checks at border crossings during Covid. In the case of coping with the pandemic and as well as with maritime cyber threats, it seems that alerting and monitoring approaches only provide a partial defensive response to the external attack vector. As opposed to this, when we examine the level of protection of this approach based on international cyber protection standards for OT systems,[28] it appears that this approach provides only a basic level of protection (SL-1), as detailed in Table 1 below, in accordance with the standard published in 2018 by DNV-GL, and contains the ISA/IEC 62443 (International Electrotechnical Commission) standard, which is used as a cybersecurity standard in automation and control systems in the oil and gas industry for OT systems embedded in the maritime industry.

Table 1: The definition of protection levels vs. protection capabilities and the nature of threat

Security Levels	Defense Capabilities vs. the Nature of the Threat
SL-1	Protection against casual or coincidental violation
SL-2	Protection against intentional violation using simple means, low resources, generic skills, low motivation
SL-3	Protection against intentional violation using sophisticated means, moderate resources, IACS specific skills, moderate motivation
SL-4	Protection against intentional using sophisticated means, extended resources, IACS specific skills, high motivation

The third approach is based on active defense software installed on each of the OT systems and used as an "individual vaccine",[29] which can also be described as "inside-out protection". As illustrated in Figure 9, this concept focuses on the implementation of

28 International Electrotechnical Commission (ISA/IEC) 62443, *Security for industrial automation and control systems*, Part 4-1: Secure product development lifecycle requirements (2018); DNVGL-CP-0231 Cyber security capabilities of systems and components (2018).

29 Rossi et al., Cyberdefence of Offshore Deepwater, 2021.

preventive and active defense software in each of the OT systems across the maritime platform, thus providing a defensive response to both attack vectors (external and internal), and providing the highest level of protection against state-sponsored attacks (SL -4). This approach does not require system upgrades, regular updates, training and prior cyber knowledge, it is suitable for the protection of connected or stand-alone, obsolete and new operating systems and allows the original equipment manufacturers (OEMs) to install it quickly and independently (between contracts). This is equivalent to the Covid-19 pandemic, when the individual Covid vaccine was developed and implemented, which can also be described as "inside out protection", as a dramatic decrease in the number of patients, infection and the danger was noted as a result, and allowed medical professionals and leaders to determine that this was the most appropriate way to cope with the pandemic.

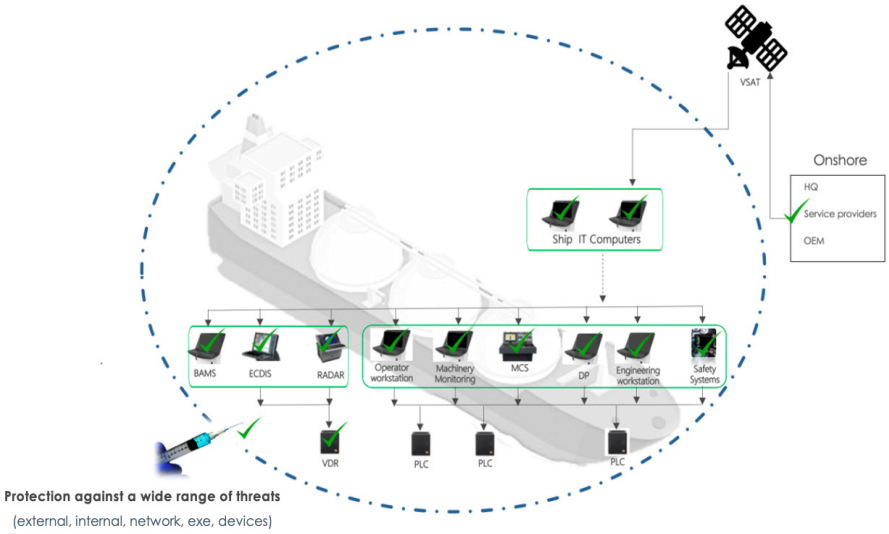

Figure 9: The "inside out" defense approach on a maritime platform

Conclusions and Recommendations

This article's main findings indicate that over the past decade, civilian maritime platforms have become increasingly dependent on OT systems, based, for the most part, on obsolete operating systems with no security updates, limited monitoring capabilities, and usually no cyber protection. These technological shortcomings turn the OT systems into a weak point from a cyber perspective, with a basic level of protection (SL-1) that is not suited for coping with the growing widespread, sophisticated threat. These conditions create a real danger to maritime platforms operating, sailing, and docking in Israeli ports and Israel's

waters (territorial and economic [EEZ]), and may lead to considerable consequences at strategic, security, economic, environmental, and national levels.

It is recommended that the various decision-makers and representatives of the maritime industry in Israel (regulators, commercial vessel owners, shipping companies, energy companies and seaports) re-examine the level of cyber threat faced by each of the various components of the maritime industry against the level of cyber protection that exists for the platforms operating infrastructures in Israeli waters. Furthermore, it is recommended that the decision-makers in Israel adopt the ISA/IEC 62443 cyber standard for quantifying threats and defining the required level of protection (Security Levels – 1, 2, 3 and 4), rework the regulation definitions accordingly, and make sure this regulation is mandatory, and carry out more extensive and thorough cyber protection inspections for owners of maritime platforms (shipping and energy companies) operating in Israel's seaports and Israeli waters (territorial and economic [EEZ]). Finally, a work plan for national preparedness on how to cope with cyber-attacks on maritime platforms operating within Israel's borders, which may lead to loss of human life and danger to the environment, economy, and security, should be developed.

Itai Sela, is a PhD candidate at the University of Haifa business school, a researcher at the Maritime Policy & Strategy Research Center, University of Haifa, and the CEO of Naval Dome cyber defense solution for maritime platforms. Itai served as a naval commander and has 25 years of experience in the Israeli Navy, holding numerous field and HQ commanding positions. He holds a BA in Social Sciences from Bar Ilan University and an MBA from Ben Gurion University.