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

Section 6: Crisis Management and Technology in the Maritime Domain

The three articles in this section discuss various aspects of threats and opportunities in the maritime domain and how they may be managed. The first article discusses the need to establish Whole-of-Government frameworks to take in the various organizations involved in Israel's maritime domain, in order to share information and streamline each entity's response time and use of its abilities. The article presents several models of existing frameworks in other countries, and it is possible to learn from their experiences to establish similar frameworks in Israel in order to improve the nation's readiness for emergencies in the maritime domain and ability to handle them better and more efficiently. The second article provides an overview of the threat of cyberattacks against maritime platforms and explores how states can and must prepare for them. It presents the full scope of the threat and the damage that cyberattacks on maritime platforms can inflict, and it proposes solutions that would be hugely expensive but are required for effective and proper cyberdefense, in order to put them into practice and not leave them as mere recommendations. The third article discusses the economic, regional, and strategic opportunities for Israel in the present era in the field of ship construction. Israel can develop, for example, unmanned surface vehicles and autonomous ships. Israel enjoys a technological advantage in many fields that may be leveraged for the economic development of the country in general and of the Haifa and northern region in particular, and to enhance Israel's soft power in these fields. Such a "blue economy" could foster regional cooperation. On a strategic level, Israel has an opportunity to shake off its "maritime blindness" and create the conditions to boost its influence on the international stage.

Whole-of-Government Frameworks for Maritime Security

Eleanor Dayan

On the morning of February 17, 2021, the State of Israel woke to a large-scale ecologic disaster when thousands of tons of tar spilled to its shores, in an event that was known in Israel as "Zefet Ha'seara" (literally translated to English as Tar of the Storm), known worldwide as the 2021 Mediterranean oil spill.[1] Preliminary investigations indicated that the tar originated from a vessel sailing off coast of Israel, which was considered as the prime suspect. However, since the event no one took responsibility for the damage to the ecosystem and the cleanup expenses. Consequently, the Israeli Minister of Environmental Protection (at the time), Gila Gamliel, instructed the Sea Pollution Prevention Fund to use its budget to finance the emergency clean-up operations.[2] On the second day of the event, hundreds of experienced teams and volunteer groups arrived at Israeli beaches to minimize the damage for the 160 km strip as much as possible. Several of the volunteers were hospitalized due to intoxicated tar fumes, which was only one of the oversights in the event.[3] Minister Gamliel claimed that since 2008, the government has neglected to legislate a national response and preparedness program for marine pollution, which includes NIS 15 million to establish a maritime intelligence monitoring system to alert against sea pollutions. Moreover, the legislation would require local authorities to prepare for sea pollutions with proper equipment and additional staff for the responding teams. In May 2021, a memorandum regarding those issues was published and closed for comments, but has not been discussed in the Knesset since.[4] To add insult to injury, the investigation of the event revealed that on February 11 (six days before the tar arrived on the shores), international agencies had already spotted the massive oil spillage merely 50 km from the coast of Ashdod.[5] It was discovered by a European Union Space Agency satellite. Although not a member of the European Union, Israel could have purchased the

---

1 Shani Ashkenazi, "From the North to Rishon Lezion: Big Amounts of Tar Spill to Israel's Shores", *Globes*, February 17, 2021 (Hebrew).

2 Shani Ashkenazi, "Black Ecological Disaster: Tar Spill to Israel's Shores, Cleaning Operation Began", *Globes*, February 18, 2021 (Hebrew).

3 Carmel Libman, "Tar Pollution in Israel's Shores: Several Hospitalized, Ecological Emergency", *N12*, February 20, 2021 (Hebrew).

4 Ilana Curiel, "Knesset's Report: Israel is Not Prepared to Sea Pollution", *Ynet*, February 28, 2022 (Hebrew).

5 Yuval Bagano, Moshe Cohen, "The Ecological Disaster at the Shores: After the Damage, Now the Many Failures Are Revealed", *Ma'ariv*, February 21, 2021 (Hebrew).

satellite services or even develop its own capabilities.[6] A channel 13 News investigative report revealed that out of the ten suspected tankers, the one with the highest probability of being responsible to the event was involved in a similiar incident in 2008 in an oil spill off the coast of Denmark.[7] This example demonstrates that such events could be better managed with the proper information and resources.

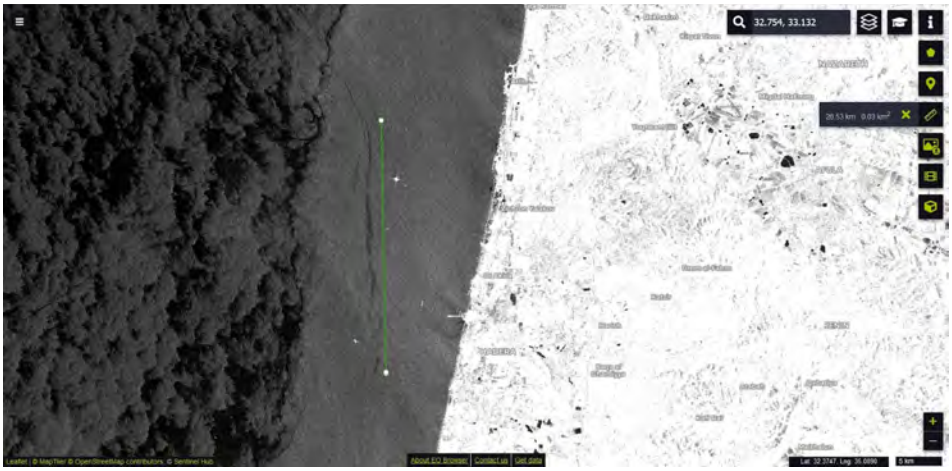

Figure 1: Satellite photo of the 26.4 km long tar spillway, approximately 10 km from Hadera.[8]

The pursuit after maritime security is confronted by high complexity of threats at sea due to wide variety of possible scenarios which require extensive information gathering capabilities and effective response procedures that can coordinate between large number of stakeholders. This article discusses whole-of-government frameworks for maritime security; an approach designed to oversee threats and challenges, optimize responses to events, and coordinate them between relevant organizations. In practice the approach is realized in its core a specialized governmental unit that operates independently or under one of the government's ministries. First, I'll provide the theoretical background for a whole-of-government framework for maritime security. Second, I'll present examples from around the world, specifically it will present the frameworks of the United Kingdom, Singapore, Australia, and New Zealand. Lastly, I'll examine the importance of a framework

6 Anat Roe, "The Tar Disaster in the Shores: Israel Could Have Prevented Some of the Damage", *Calcalist*, February 21,2021 (Hebrew).

7 Yoav Zehavi, Chen Beyar, "One of the suspected ships in the pollution was involved in a major oil leak 13 years ago", *Kan*, February 22, 2022 (Hebrew).

8 Illustration source: Sue Surkes, "Satellite images of oil slicks off coast show recent spill far from a one-off", *The Times of Israel*, February 28, 2021.

in a case study of Israel, and determine which of the principles and lessons from the other case studies decision makers should consider when designing such frameworks.

Whole-of-Government Frameworks for Maritime Security – Theoretical Background

There is no single definition for maritime security. It can be interpreted as the absence of threats in the maritime domain, including terrorism, disasters, accidents, illegal trade, and environmental damage. It can also be defined as an aspiration for the stable order of the sea, or as the sum of actions such as protecting ships, ports and the marine environment.[9] One thing is clear though, achieving it and dealing with threats require the participation and cooperation of many organizations (government, private and international), broad knowledge of multiple issues, and the ability to respond quickly to complex events. In this complicated reality where many players have to participate in order to bring about a desired result, a body that can manage or at least coordinate such joint efforts is required.[10] The process of confronting maritime security threats should include four stages: identifying events and threats in real time; monitoring, assessing and knowledge sharing regarding the situation as it develops; deploying quick response forces and resources; and lastly, assessing the damage and forming a restoration plan.[11] Each of the stages requires collection and verification of information, coordination between several entities, an understanding of the legal and political circumstances, ability to plan and execute initial response, and drawing conclusions and implementing them in relevant organizations. A whole-of-government framework for maritime security is designed to achieve all of these.

The complex nature of maritime security threats raises some unique issues. Even though a head of state or a parliamentary committee can direct and coordinate responses in a way that serves the interests of the state, it cannot be expected of them to get immediately involved in each case and security issue, such as handling detainee and detained cargo cases, collecting evidence, contemplating the right to board a ship at sea, or designing press releases. This problem stems from the increasing speed of that the transformation of information that could change policy. The amount of information and the need to

---

9 Christian Bueger, "What Is Maritime Security?" *Maritime Policy*, 53, no. 1 (2015): 161–164.

10 Duane M. Smith and Thomas C. Fitzhugh, *International Perspectives on Maritime Security* (Washington D.C: Department of Transportation, 1996), 1–4; Brett Doyle, "Lessons on Collaboration from recent conflicts: The Whole of Nation and Whole of Government Approaches in Acting", *Inter-Agency Journal*, no. 1, (2019), 105–122.

11 Ido Ben-Moshe and Ehud Gonen, "Sea pollution: How to prevent the next disaster", *The Geostrategic Series* (Haifa: Chaikin Chair for Geostrategy, University of Haifa, 2022), 61–67 (Hebrew).

disperse it quickly, along with the intricacy of the events in the maritime domain means that first responders are sometimes unable to share real time information from the field up in the hierarchal chains fast enough with the responsible decision-making authorities. Hence, an organization which can fill this gap is required. The increasing need for broad knowledge and different respond expertise regarding situations such as fuel leakages or other materials, piracy, damage to energy infrastructure, or illegal trading, fishing, and immigration, has worsened the problem, and without existing protocols to coordinate the responding efforts, misinformation and inefficiency may result in repeating past mistakes.[12] As written:

> "No single agency owns maritime security or can manage their specific maritime threats without the support of other agencies and stakeholders such as the community and industry. Our ability to understand, engage with partners, and prevent and respond to maritime threats is built upon the foundation of a cohesive multi-agency approach that draws together and utilises the full range of national capabilities."[13]

This Whole-of-Government Approach (WGA), also known as "Comprehensive Multi-Agency Approach" is intended to combine joint efforts of government organizations in order to fully utilize resources in a coordinated response to events. At the center of the approach there is the understanding that without cooperation and coordination every organization will only focus on its own interests and goals. The integration of information and capabilities will allow more response options, efficiency, and less dependence on certain entities (like the Navy).[14] This approach aims to improve effectiveness by integrating knowledge, resources, and capabilities of various organizations. Moreover, WGA leads to a systematic understanding of the complexity of threats, and therefore assigns experts from different fields to respond to them. The shared use of resources and information is intended to reduce costs and increase efficiency.[15] A Whole-of-Government Framework (WOGF) integrates entities within the government and responds to several challenges, among them, achieving maritime operational capabilities, increasing responding organizations' resources, holding discussions, coordinating efforts and decision making

---

12 Brian Wilson, "The complex nature of today's maritime issues: why whole-of-government frameworks matter", In Joachim Krause and Sebastian Bruns (eds.), *Routledge Handbook of Naval Strategy and Security* (New York: Routledge, 2016), 153–156.

13 Ministry of Transport, "Maritime Security Strategy", New Zealand Ministry of Transport, December 2020.

14 Terry A. Fellows Jr & Jason L. Percy, *A whole of government approach for national security*, 4 (MBA professional report, Naval Postgraduate School, Calhoun, 2009), 17–19.

15 Andrea Baumann, *Whole of Government: Integration and Demarcation* (Center for Security Studies, ETH Zurich, 2013), 1–4.

between ministries in the government and outside it, and establishing procedures for collecting and verifying information. An existing crisis management procedure allows security organizations, both governmental and non-governmental, to prepare responds to events, compensate for early event uncertainties, document the lessons learned, and implement them in organizational procedures afterwards.[16]

The success of the multi-agency approach relies on effective maritime security system enablers.

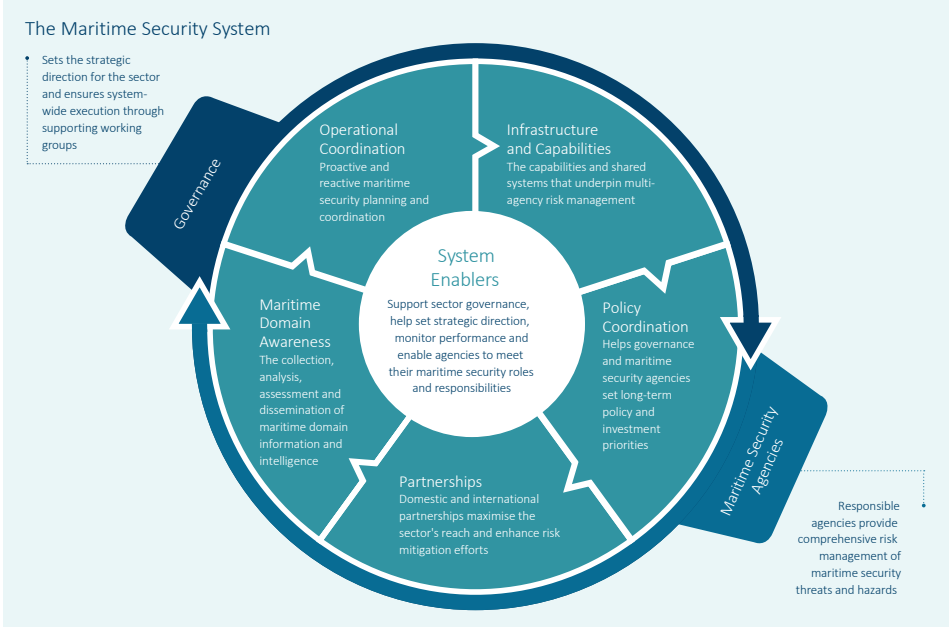

Figure 2: Maritime Security WGA in New Zealand.
(Source: Maritime Security Strategy 2020)

Whole-of-Government Frameworks for Maritime Security Around the World

Dealing with complex threats to maritime security is fairly new and it has been developed in recent years, along with the information age and its increased flow of data. Since the beginning of the 21st century, governments around the world started establishing WOGF for maritime security, and as it turns out, the two main reasons for their existence in these countries are the size of their maritime domain and its national importance. Notably, the framework's role in each country is different and determined by the threats, constraints, and unique characteristics of each domain. I will start by introducing Singapore as an

16 Wilson, "The complex nature of today's maritime issues", 2016.

example of a small state, functioning as an island nation (its main gateway to the world is by sea or air, especially for importing and exporting of trade), much like Israel, and with similar economic capabilities. I'll focus on the center's ability to gather information in the complex space of the Singapore Strait. Following, I will discuss the case of the United Kingdom as a country, whose maritime domain has immense importance for centuries, but its Maritime Security Coordination Centre was established only in 2020. I will examine the organizational position of the framework as a jointly budgeted and staffed governmental entity. And finally, I will present a comparison of New Zealand and Australia and examine authorization issues of the framework as a coordinator, on the one hand, and an operational maritime security organization, on the other.

Singapore

At the heart of Singapore's National Maritime Security System stands the Singapore Maritime Crisis Centre (SMCC). Established in 2011, it coordinates its activities through the Crisis Management Group which is led by the Commander of the Navy. The Centre operates under the authority of the secretary generals of the ministry of defense and the ministry of interior under the Homefront Crisis Executive Group. The SMCC optimizes interoperability between various organizations by assessing and reporting on potential threats, planning crises responses, managing and supervising operations in real time, developing capabilities, and conducting training. The center stands on three pillars: The first is a body of representatives from various maritime organizations, including the Singapore Navy, the Maritime and Port Authority of Singapore, the Immigration and Checkpoints Authority, the Police Coast Guard, and Customs. The center went fully operational in 2013 and since then coordinated with intelligence agencies, think tanks, and shipping companies.[17] The second pillar is the National Maritime Sense-making Group (NMSG), which uses artificial intelligence and multi-sourced data analysis to create security profile of every vessel passing through Singaporean maritime domain, and identifies potential threats, anomalies, and suspicious behavior. The system is linked regularly to databases of intelligence services, shipping companies, and organizations in the shipping sector. The group shares these assessments with the relevant authorities who in turn verify the information and inspect the vessel.[18] The third pillar is the National Maritime Operations Group (NMOG), which conducts training, writes protocols, and analyzes lessons learned to improve performance and coordination during a crisis or a threat. At such a time or during simulations, the center will coordinate the methods of

17 Ministry of Defense, "Fact Sheet: Singapore Maritime Crisis Centre (SMCC) and Launch of SMCC Next-Generation Maritime Sense-making System", *MINDEF Singapore*, November 12, 2021.

18 Ibid; Nicholas Lim & Chong De Xian, "Maritime Sense-Making and The Role of Big Data Analytics for Enhancing Maritime Security", *PONTER Journal* (September 2020).

response and prevention between the Maritime Security Task Force of the Singapore Navy and the relevant organizations.[19]

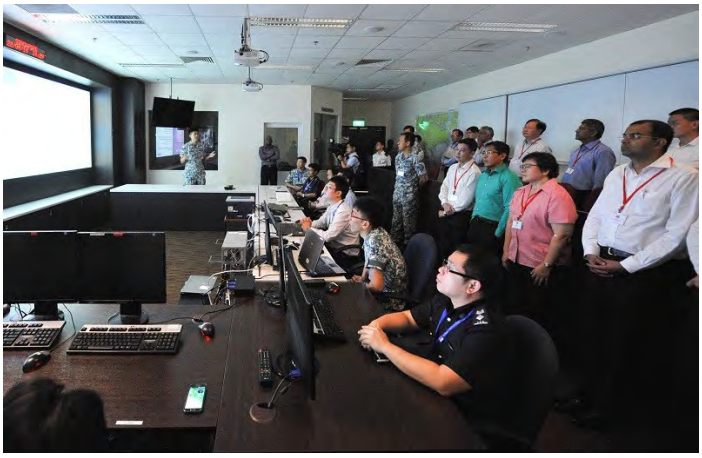

Figure 3: Singapore's foreign affairs and defense committee visits the Singapore Maritime Crisis Center (SMCC). (Source: *MINDEF Singapore* 2014)[20]

Among the notable threats that the center identified and intercepted was the 2014 identification of a crew member who was listed on two ships destined to enter Singapore the same day. With threats of an attack by a faction of ISIS in Sri Lanka in the background the NMSG shared the information and thus prevented his entry.[21] In 2015, the AI system identified a potential ISIS supporter on board a tanker destined to the port of Singapore, who as a result was forbidden to leave the ship. In 2016, the Centre identified a suspicious ship, the Police Coast Guard detained the ship and found smuggled goods aboard it. One of the crew members was arrested following the incident.[22] The main aspect to be learned from the Singapore case study is the ability to collect quality information through framework procedures. The Singapore Strait is the busiest sea passage in the world and the port of Singapore is the second busiest. An average of 1,000 vessels sails the 1,067 square kilometers of Singapore's Exclusive Economic Zone at any given time, and a vessel enters or leaves every two to three minutes. The ability to get a clear picture of what is

19 Ministry of Defense, "Fact Sheet: Safeguarding Singapore's Maritime Security", *MINDEF Singapore*, June 30, 2017.

20 News Releases, "Government Parliamentary Committees Visit Singapore Maritime Crisis Centre", *MINDEF Singapore*, April 22, 2014.

21 Joseph Franco & Romain Quivooij, "Terrorist Threats from the Maritime Domain: Singapore's Response", *RSIS*, No. 197, October 10, 2014.

22 Ministry of Defense, "Fact Sheet", 2017.

happening in the maritime domain and to react to threats on time is a central pillar of the whole-of-government approach for maritime security.[23]

The United Kingdom

The importance of maritime security, whether it is for international trade, economic growth, or global law and order, is nothing new to the United Kingdom. The National Strategy for Maritime Security (NSMS) from 2014 recognizes that maritime security deals with diverse issues and not only naval superiority, and outlines for the first time in British history the importance of a whole-of-government approach. The Joint Maritime Security Centre (JMSC) was established in 2020 as part of the effort to coordinate between the National Maritime Information Centre (NMIC) and the Joint Maritime Operations Coordination Centre (JMOCC). The JMSC is the interorganizational executive body that implements the whole-of-government framework for maritime security in the UK, and is responsible for maintaining maritime knowledge, responding to security threats, and conserving the marine environment.[24]

The Centre's main tasks are to raise level of preparedness for maritime threats and to coordinate government responses. It is led by a team of representatives from the Royal Navy, the Ministry of Defence, the Border Force, the Marine Management Organization (MMO), with the Centre's board of directors above them. The JMSC coordinates other government authorities as well, including the Ministry of Transportation, the Foreign, Commonwealth and Development Office, the Ministry of the Interior, British Customs, the British Coast Guard, the National Crime Agency, the Counter Terrorism Police, and Maritime Scotland. The JMSC provides a number of services to the British government and other organizations, such as collecting and analyzing security information and constructing a coherent picture of the occurrences in the maritime domain; planning and coordinating responses between organizations, their assets, and their capabilities. Similar to the Singaporean model of whole-of-government framework, the British Centre consists of three components; the executive team that was mentioned before; the National Maritime Information Centre (NMIC), established in 2017, provides data analysis, intelligence and crisis management to maximize the capabilities of operational responders; and the Joint Maritime Operations Coordination Centre (JMOCC) that monitors the United Kingdom's maritime domain around the clock using advanced technologies and a team of

---

23 Nicholas Lim and Chong De Xian, "Maritime Sense-Making and The Role of Big Data Analytics for Enhancing Maritime Security", *Pointer, Journal of the SAF*: 1–10 (September 2020).

24 Scott Edwards, "The United Kingdom's Conceptualization of Maritime Security", *Asia Maritime Transparency Agency*, March 4, 2022; Cristian Bueger, Timothy Edmunds & Scott Edwards, "Innovation and New Strategic Choices", *The RUSI Journal*, 166, no. 4 (2021): 66–75.

government representatives that identify threats and incidents at sea, and coordinate naval and aerial responses.[25]

In addition to information gathering and a variety of resources and capabilities, the British Centre is unique for its independence from any ministry or other government authority. The Centre is jointly staffed and budgeted by organizations sharing its maritime space objectives, including the Royal Navy, the MMO and the Ministry of Defence. This allows each of the organizations to work in equal conditions resulting in improved cooperation and coordination in those situations that are coordinated or managed by JMSC.[26] For example, the Royal Navy annually purchases satellite-based intelligence services from Airbus for the JMSC, providing the Centre with a broad maritime domain awareness of the British waters, therefore allowing quick responses to possible threats.[27] Although independence from any particular ministry seems like an organizational mess, interestingly enough, having been established relatively late, the British Centre chose to set the framework in that order, after considering lessons from previously established centers.

Figure 4: The Thai Ambassador to the UK visits the JMSC.
(Source: Royal Thai Embassy, London 2021)[28]

25 HM's Government, "Joint Maritime Security Centre" (Accessed August 6, 2022).

26 Scott Edwards, "Safe Seas Visits UK's Joint Maritime Security Centre", *Safe Seas*, October 12, 2021.

27 Press release, "Airbus to provide satellite-based maritime surveillance services for the UK Royal Navy", *Airbus*, June 28, 2021.

28 "Thai Ambassador visited the Joint Maritime Security Centre and National Maritime Information Centre in Portsmouth", *Royal Thai Embassy, London*, September 8, 2021.

New Zealand and Australia in Comparison

A review of the government of New Zealand from early 2001 that examined the necessary resources required for military and civilian organizations to operate in the maritime domain found that ten different government authorities were patrolling the seas independently, each one with its own interest at hand – a fact that prevented the effectiveness of information gathering in a national perspective. That same review recommended the establishment of a maritime coordination center that will manage and coordinate the country's resources and responsibilities in the maritime domain and will identify constitutional gaps that prevent effective gathering of information or patrolling the seas. The subsequential established center currently consists of a mixed team of armed forces staff and government officials, and acts as an independent body with its headquarters in a military base. The National Maritime Co-ordination Centre (NMCC) was established in 2002 and is currently budgeted by the Ministry of Customs.[29] In addition to efficient management of patrolling vessels, the NMCC collects data for systems such as automatic identification, long-range identification and tracking, vessel monitoring, customs data and geographic data from civil and government providers, combined with the data collected by the military.[30] The center uses a Maritime Anomaly Indication and Alerting tool to analyze information collected from thousands of vessels simultaneously and warn of suspicious behavior.[31] The center then passes the information to the Navy, the operating authority at sea.

Many changes in naval security occurred in Australia post 9/11, the most important of which is the establishment of the Border Protection Command in 2005. It was renamed the Maritime Border Command (MBC) in 2015, when it was subjugated to the Australian Border Force (ABF), then the newly law enforcement administration of the Australian Department of Home Affairs.[32] As it represents the whole-of-government framework for maritime security in Australia, the MBC is designed to identify, deter, and respond to

---

29 Office of the Auditor-General, "Effectiveness of arrangements for Co-ordinating civilian maritime patrols", *Controller and Auditor-General*, April 12, 2010.

30 Chris Rahman, "Maritime Domain Awareness in Australia and New Zealand", in Natalie Klein, Joanna Mossop & Donald R. Rothwell (eds.), *Maritime Security: International Law and Policy Perspectives from Australia and New Zealand* (New York: Routledge, 2009), 202–223.

31 The Defense Technology Agency – DTA, "Maritime Domain Awareness" (Accessed September 12, 2022).

32 Donald Rothwell and Cameron Moore, "Australia's Traditional Maritime Security Concerns and Post 9/11 Perspectives", in Natalie Klein, Joanna Mossop & Donald R. Rothwell (eds.); *Maritime Security: International Law and Policy Perspectives from Australia and New Zealand* (New York: Routledge 2009), 37-53.

non-military threats, and prevent illegal activity in the maritime domain by using civilian vessels and aircrafts.[33] The center engages with illegal trade or immigration, exploitation of natural resources, marine pollution, terrorism, piracy, and fuel leakages. Other than cooperating with the Australian Navy and coordinating teams and vessels of the ABF as the operations command and crisis manager, the center also collects maritime information using the Australian Maritime Identification System.[34]

The main difference between the frameworks of Australia and New Zealand (as well as the other examples given in this article) is the ability to operate independently. In the case of Australia, the center is directly assigned with vessels, aircrafts, and response teams from the Australian Army and Navy on a regular basis, while in New Zealand, the Centre depends on other organizations (The Navy mainly) to act upon gathered information. Hence, the Australian Centre is capable of conducting command and coordination activities while the Centre in New Zealand is capable of conducting only coordination ones.[35]

Figure 5: Vessel assigned to MBC (Source: shipshub.com)

Whole-of-Government Framework for Maritime Security in Israel

The 2021 Mediterranean oil spill highlighted the lack of a unified government effort to collect information and respond to maritime domain incidents, but the issue is misunderstood by the decision-makers and is still not prioritized. Despite the economic and security importance of the maritime domain to Israel, there is no national organization

33 Australian Border Force, "Maritime Border Command" (Accessed September 12, 2022).

34 Department of Immigration and Border Protection, "Maritime Border Command" (Accessed September 12, 2022).

35 Michael Blades, "Focusing New Zealand's approach to maritime domain security" (Unpublished thesis, Massey University, New Zealand, 2014).

that coordinates and responds to maritime incidents. The Israel Navy is equipped to protect the country's national security against armed threats but is unauthorized to manage non-national security scenarios, whether they be disasters, accidents, pollution, or illegal smuggling, trading, or fishing. While the issue of securing energy facilities from external threats did receive attention, the rest of the wide array of threats to the maritime domain and marine environment got pushed aside. Currently, the question of authority remains unclear and the responsibility for maritime security is divided between nine government agencies, a reality that creates many potential gaps for a unified action. The inability to determine who should respond to an incident, who should receive the necessary information to assess an appropriate response, or who should coordinate between organizations, is preventing an understanding of the bigger picture in the Israeli maritime domain, and consequently leads to ineffective utilization of government assets.[36]

Assuming that a whole-of-government framework for maritime security is considered by decision-makers to be of vital importance to the State of Israel, and as part of a larger effort to shape a national maritime strategy,[37] there are two lessons to be taught from the case studies presented in this article. The first is the importance of a comprehensive multi-sourced information system. Sources can be, for example, databases, research and academic institutes, open sources like internet databases, and also collaborations with government authorities and international organizations, and service providers like photography and satellite image analysis (as seen in the case of the United Kingdom). Additionally, there is a need for a platform to analyze, manage, and verify data, using Artificial Intelligence engines in order to produce an overall picture of the maritime domain. This issue was discussed in the *Maritime Strategic Evaluation for Israel 2021/22*, where it was shown that existing monitoring technologies are required to maximize the safety of the citizens and the maritime domain.[38] Furthermore, an apparatus that will coordinate between responding organization during an event, and plan ahead courses of action for possible scenarios is essential. According with the framework's goals and other limitations, some of the organizations that are expected to participate in these efforts are: the Israel Navy, the Israeli Police, the Ministry of Defense, the Ministry of Environmental Protection, the Nature and Parks Authority, the Ministry of Energy,

---

36 Sue Surkes, "Experts: Israel has 'no strategy' for managing 'lifeline' Mediterranean Sea", *The Time of Israel*, November 25, 2021; Shaul Chorev, "Israel must increase its maritime awareness in light of recent oil spill", *The Jerusalem Post*, March 1, 2021.

37 Further reading: Oded Gour Lavie, *A Model and Methodology for a Grand Maritime Strategy*, Maritime Policy and Strategy Research Center, University of Haifa, June 2018.

38 Semion Polinov and Shaul Chorev, "A Model for an Israeli Academic Marine Monitoring System", in Shaul Chorev and Ziv Rubinovitz (eds.), *Maritime Strategic Evaluation for Israel 2021/22* (Haifa: Maritime Policy and Strategy Research Center, University of Haifa, 2022), 333–345.

the Ministry of Transportation, the Ministry of Justice, Israel Port Authority, shipping companies, the Society for the Protection of Nature, coastal municipal authorities.

The second lesson discusses authority. The case studies in this article describe two types of frameworks, one that is capable of assigning resources, equipment, and personnel, and is able to respond to maritime threats and incidents independently (Australia), and another that only manages the accumulation of information and the coordination of resources. The first type grants authority to the framework and an ability to proactively contribute to maritime security, while the second offers streamlining and coordination between organizations but doesn't change the existing hierarchy. This issue also relates to the framework's budgetary and hierarchical independence. The decision-makers must decide if the framework is budgeted by a specific government ministry and managed by it or operates independently and jointly budgeted by the participating organizations. The first option associates the center's activities with a specific government ministry, but would bring stability to its efforts, while the second divide the costs of the framework between the contributing organizations and create equal working conditions, the same way the British center operates.

Where might be the place of a framework in the government system and how would it look like? First, a maritime security coordination center is the core of whole-of-government framework for maritime security. This center should be oriented by the cabinet and the maritime strategy simultaneously, and its actions to be overseen and evaluated by one of the Knesset's committees. The framework (and its coordination center) requires a managing team consisted of a director, representatives from the organizations essential to the center's activities (i.e., the Navy), and the groups that conduct the rest of the center's activities. The case studies teach us that one of the groups will need to assign a team to collect maritime data. The data will be forwarded to an analysis team that will update the maritime domain status, using data management systems. In addition, because the amount of accessible information is growing regularly, a third team will be charged with developing tools for verifying and analyzing that information. The second group will coordinate and manage operations and responses which include representatives from all relevant organizations. The group, alongside the management team, will prepare respond options, coordinate events and exercises, and evaluate them afterwards. The center's staff will also be involved administratively, operationally, or any other way.

In conclusion, the article introduced a whole-of-government approach for maritime security and presented countries that implemented such frameworks as part of their maritime strategy. The importance of a framework to Israel was also examined. Even though the maritime domain is more significant to those countries that currently have a WOGFs in comparison to Israel, it is still important to note that a WOGF is designed

to optimize the country's maritime security efforts, regardless of the nature of the threats. The information age presides new challenges; dealing with an enormous amount of information and a need to analyze it quickly; dealing with complicated challenges that require the intervention of many organizations; and the increased dependence on the maritime domain. As a result, new ways to face those threats are necessary. The whole-of-government framework is designed to respond to these threats and changes, and therefore the demand for such a framework and its implementation is increasing worldwide, including in Canada, the United States, India, Japan, the Philippines, Sweden, the Republic of Cabo Verde, the United Kingdom, Australia, Singapore, and New Zealand.[39]

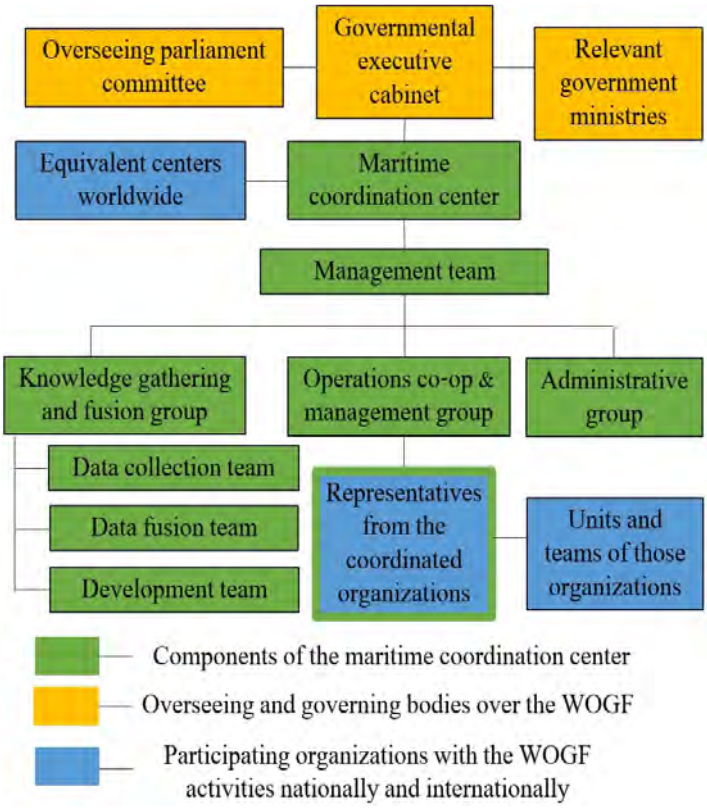

Figure 6: A proposal for an organizational structure of a whole-of-government framework for maritime security.

39 Wilson, "The complex nature of today's maritime issues", 2016.

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]

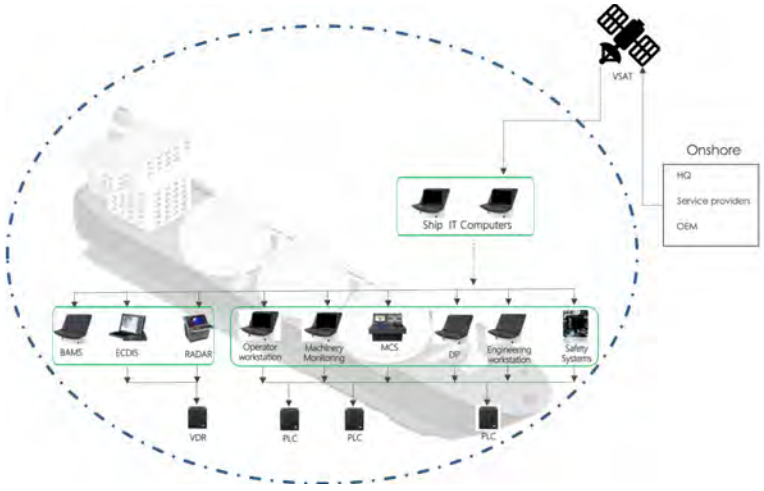

Figure 1: The layout of main OT systems in a commercial vessel

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]

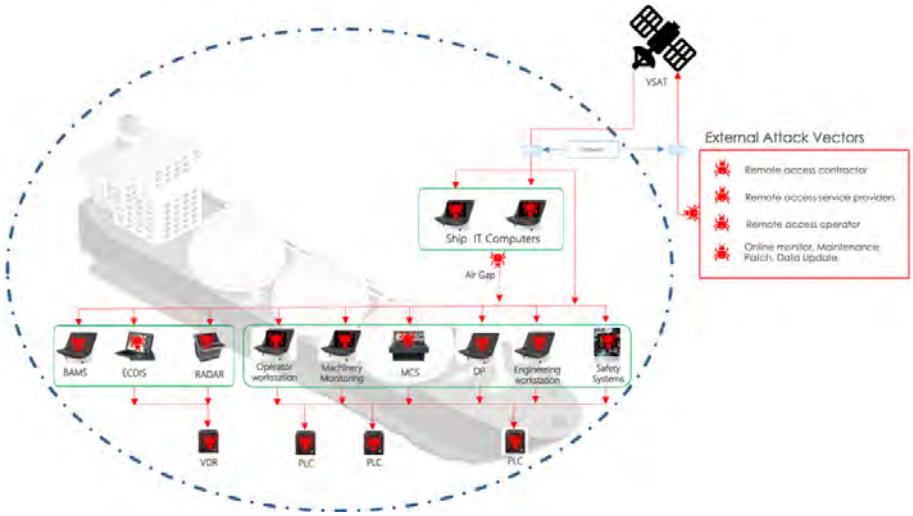

Figure 2: External attack vectors on vessels, and a description of the spread of malware from the IT systems to various OT systems

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]

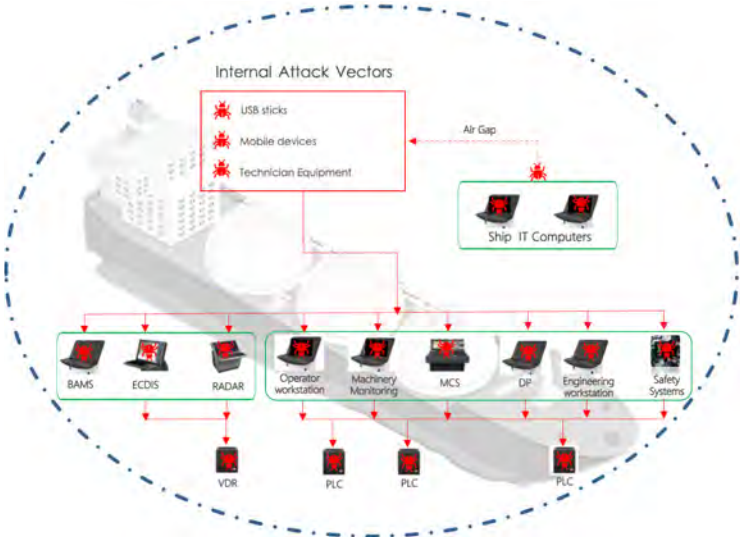

Figure 3: Internal attack vectors in vessels and the spread of malware to all OT systems

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]

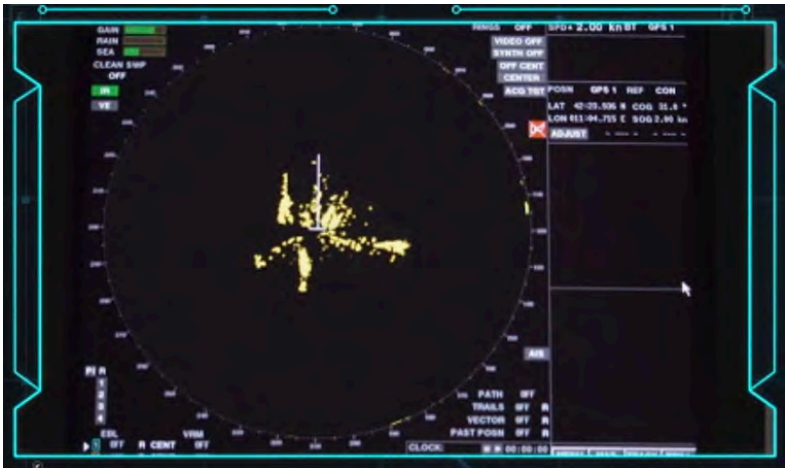

Figure 4: The RADAR display presented to the navigation officer on the bridge

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.

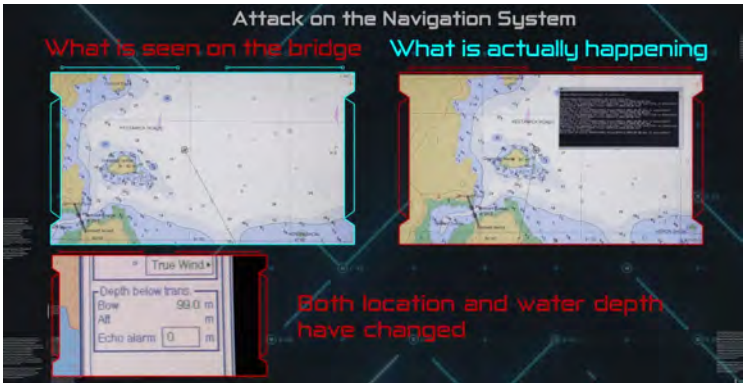

Figure 6: A Manipulation attack on the navigation system (ECDIS)

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.

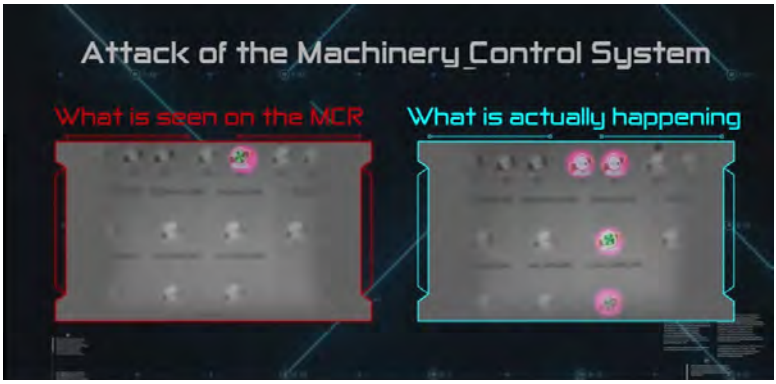

Figure 7: A Manipulation Attack on the Machinery Control System (MCS)

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]

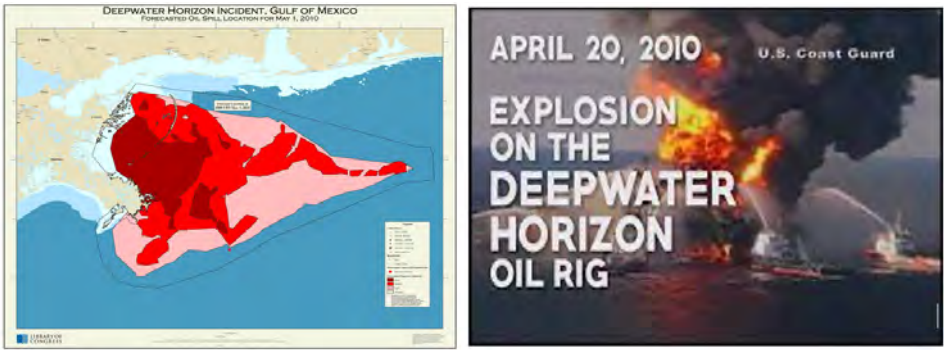

Figure 8: The 2010 "Deepwater Horizon" oil spill in the Gulf of Mexico

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.

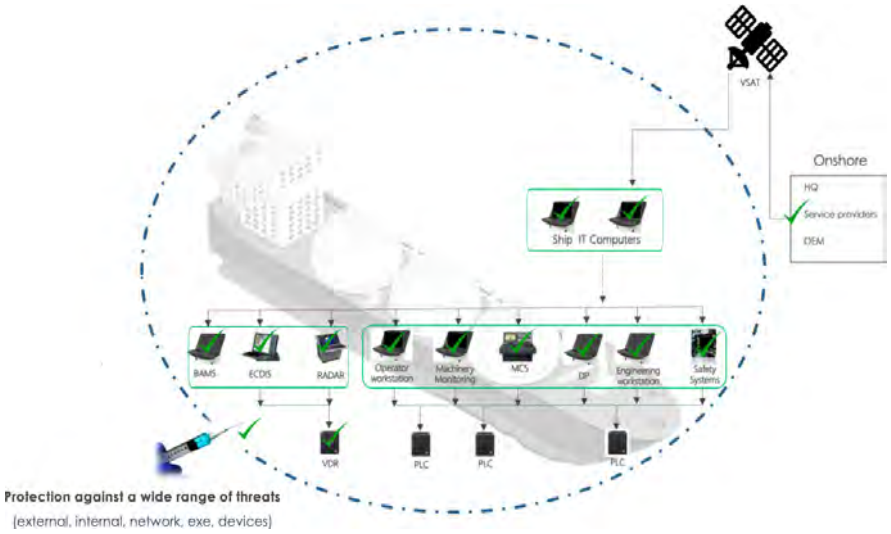

Figure 9: The "inside out" defense approach on a maritime platform

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.

Disruptive Technological Changes in the Field of Shipping and Ports as an Opportunity for Israel[1]

Ehud Gonen

The shipping sector, and parts of the maritime logistics industry related to it, are included in the 'blue economy' sector,[2] i.e., economic activity related to the sea.[3] The development of maritime technologies has been described by the OECD as one of the key factors in the development of a blue economy. In a detailed report published in 2016, predicting the development of blue economy until 2030, the organization notes a series of technologies such as sensors, satellites, autonomous systems and big data that are merging into new formations, changing the face of blue economy, and specifically shipping, navigation, maritime transport and "the smart ship".[4]

It should be noted that the field of shipping and ports is relatively conservative and operates according to global regulations, including large investments of capital. This is one of the reasons that this field experienced a relatively late digital revolution, and the introduction of disruptive technologies only during the past decade. The global bodies that regulate shipping, and especially IMO – the International Maritime Organization, have been working in recent years to create a regulatory framework for the introduction of new technologies, including autonomous technologies, into the field. Even so, the issue of advanced technologies for shipping has not yet been established according to clear international standards, and clear technological leadership of one company or another is

---

1 This article is based on a research paper 'Determining Feasibility for a Test Area for Autonomous Vessels in Israeli Waters and its Future Expansion to the Area between Israel and Cyprus', prepared for the National Economic Council at the Prime Minister's Office (Hebrew).

2 The European Union divides the blue economy sector into six branches: (a) maritime traffic and shipping, (b) food, nutrition, health and system services, (c) energy and raw materials from the sea and the seabed, (d) leisure, recreation and residences, (e) protection of beaches and cliffs, (f) monitoring, conservation and control. See: United for Mediterranean.

3 For a comprehensive overview of blue economy in Israel: Ehud Gonen, Overview of Blue Economy in Israel – Current Situation and Opportunities, Maritime Policy & Strategy Research Center (Hebrew).

4 "The Ocean Economy in 2030, *OECD*, 2016, pp. 119–126, 128–130: "These include Automated Identification System (AIS), Electronic Chart Display and Information System (ECDIS), Integrated Bridge Systems/Integrated Navigation Systems (IBS/INS), automatic radar plotting aids (ARPA), radio navigation, long-range identification, and tracking (LRIT) systems, Vessel Traffic Service (VTS) and the Global Maritime Distress Safety System (GMDSS). Moreover, ships now carry global satellite navigation systems (GNSS) and will soon all have reliable ECDIS".

not yet evident. For this reason, the distinct technological changes that have taken place in the field of shipping in recent years are an opportunity for Israel on a national level.

This article addresses the implications for Israel related to technological developments in the field of commercial shipping and maritime logistics. These developments include opportunities for Israel on three levels: economic opportunity: autonomous shipping technologies as a catalyst for growth and employment, both nationally and for the city of Haifa and the northern region, a regional opportunity: blue economy as a platform for regional cooperation in the eastern Mediterranean and the northern Red Sea, and a strategic opportunity: maritime technology as a tool for disillusionment from Israel's "maritime blindness", as a tool for increasing Israeli soft power, which can be an opportunity for possible Israeli influence on the international community. In addition, shipping technologies, and especially 'autonomous shipping' related to international trade, enable the collection of information and influence related parties beyond the specific field of shipping.

Economic Opportunity

On a national level, Israel is internationally known for its local ecosystem in the fields of technological innovation to the point of branding the country a "startup nation".[5] Even in the 1990s, Israel was a global leader in the field of unmanned aerial vehicles (UAVs). While many are proud of this fact, as the Biblical proverb goes, For riches are not forever', and the development of an ecosystem for new fields must continue. The coming years are a window of opportunity for Israeli industry, with a possibility of taking over a significant part of the global shipping industry market, as it has done with UAVs, the space industry and autonomous terrestrial vehicles, and beyond its relative impact on world economy or trade.

In the context of transportation, two noticeable parallel national initiatives have occurred in Israel in recent years, promoting elite technology in the fields of unmanned vehicles in the air and on land. In the field of aviation, the Civil Aviation Authority at the Ministry of Transport in Israel authorizes unmanned aircraft to fly in civilian airspace. Israel is the first country in the world to approve such activity. This, as the Hermes Starliner UAV manufactured by Elbit, which is considered the most advanced of its kind, received a civil aviation license, completing its compliance with the international (NATO) standard conditions for the integration of UAVs in civil aviation areas. It should be noted that the approval of this move by the Civil Aviation Authority enables significant economic

5 Dan Senor and Saul Singer, *Start-up Nation: The Story of Israel's Economic Miracle* (New York: Twelve, 2009).

possibilities for the UAV manufacturer (Elbit), which has already signed contracts to supply the Hermes Starliner UAV to the Swiss Federal Department of Defense, Civil Protection and Sport and the Canadian Ministry of Transport and supplies the Hermes UAV to more than ten other countries.[6]

Furthermore, in January 2021 the "Drone Initiative" was launched by the Israel Innovation Authority. During this experiment, drone flights are carried out over residential areas in Tel Aviv-Jaffa, Ramat Sharon, Herzliya and Hadera,[7] and will be operated in Brazil as well, using the same Israeli control system. Together, the participating companies are expected to perform about 300 flights a day over open areas, and perform various types of missions on air routes assigned by the joint control system.[8] This is a joint venture of many commercial companies together with the Israel Innovation Authority, the Civil Aviation Authority at the Ministry of Transport, the Ayalon Highways Company and the relevant municipal authorities. Additionally, the first drone field in Israel is being established in Yeruham.[9] This combined activity of government authorities, commercialization of military technologies, government companies and private companies, according to a suitable regulatory framework, are catapulting the field forward on a global level.

Autonomous vehicles are another relevant field. Here too, Israel is a global leader when it comes to certain systems, a status reached thanks to an entrepreneurial culture, military investments, and appropriate governmental and regulatory programs. In 2017, a national plan for smart transportation was announced. The first part of the plan is "Promoting the establishment of an autonomous vehicle testing center that supports smart transportation."[10] Over the years, hundreds of companies in the field of smart transportation have been established in Israel, some of which, such as "Mobileye", are world-class leaders in their field.

The Department of Smart Transportation at the Ministry of Transport, in cooperation with the Ministry of Transport and other relevant government agencies, is making efforts to initiate, assist and promote activities that will advance the operation of autonomous

---

6 "A Global Aviation Revolution", Ministry of Transport, February 13, 2022 (Hebrew).

7 "The National Drone Initiative Began with a Pilot over the City of Hadera", *TechTime*, June 30, 2021 (Hebrew).

8 "The Third Phase of the National Drone Project is Underway", Israel Innovation Authority, October 12, 2021 (Hebrew).

9 Keinan Cohen, "The Demand for Experiments has Taken Off, and the first Drone Field in Israel will be Established in Yeruham", *Walla News*, April 8, 2021 (Hebrew); Nurit Sommer, "A Unique Test Field for Drones Will Soon be Established Near Yeruham", *YNET*, December 20, 2020 (Hebrew).

10 "The National Plan for Smart Transportation", Government Resolution No. 2316 of January 22, 2017 (the 34th government led by Benjamin Netanyahu).

vehicles.[11] The Ministry of Transport notes that among the actions taken for this purpose are the passing of the 'Law on Autonomous Vehicle Experiments in Israel', and the preparations for sub-legislation on the matter (the law entered into effect in April 2022).[12]

In the context of innovation and development, the National Economic Council at the Prime Minister's Office stated:

> Leveraging technological innovation in Israel: While Israel has not been a player in the traditional automobile industry until now; it is emerging as a major player in the field of smart transportation, where it has a comparative advantage. The transition from the development stages to the implementation stages of smart transportation creates another significant opportunity for Israel, which can also become the focus of beta sites.[13]

This Israeli technological leadership in the fields of aviation and autonomous vehicles, as well as in the field of space (not detailed in this document) was achieved even though Israel does not have a distinct production of terrestrial or aerial platforms.

In the past decade, there are indications of a substantial change in the way the shipping and ports sector operates, and it is possible to identify a number of operational areas in which a substantial change is taking place. The first is process automation and autonomous shipping. Another trend related to automation is the development of cyber for the maritime domain, and the third is big data. Israel has distinct bodies of knowledge and development capabilities in all of these fields. Thus, there is room to expand activity in the fields of space, air and land technologies to the sea as well.

Process automation and autonomous shipping: Difficulty in recruiting shipping personnel and a wish to reduce ship operating costs are pushing the industry to cut down on crews by introducing advanced technology in the fields of navigation and ship operation. This is related to the remote operation of ships from offshore control centers or completely autonomous shipping on fixed lines, such as ferry lines, supply to fixed rigs at sea, and the like.

Cybersecurity: the emergence of cyber warfare and the increasing involvement of state and non-state actors in cyber-attacks on critical infrastructures such as ports, both in

---

11 "Autonomous Vehicle", Ministry of Transportation, April 5, 2021 (Hebrew).

12 "The Knesset has Begun Debating a Bill that will Allow Conducing Tests on Autonomous Vehicles for the First Time in Israel", Ministry of Transportation, December 8, 2021 (Hebrew).

13 Roni Bar, "Israel is Preparing for the Smart Transportation Revolution: Autonomous, Electric Vehicles, the Economic Consequences of Connected and Collaborative", Economic Council, Prime Minister's Office, April 2019 (Hebrew).

terms of information technology and in terms of operational technology, and in the process the use of private entities and advanced technologies in order to achieve strategic value, all turn the maritime domain into a most vulnerable arena. In the past decade, the civil maritime industry (shipping industries, vessels, passenger ships, shipyards, ports, terminals and gas and energy infrastructures) has become very dependent on computer and control systems based on operational technologies. These systems are mostly based on outdated operating systems, without security updates, have limited (if any) monitoring capabilities and most have no cyber protection at all.[14]

Big data for the maritime sector: in the maritime sector, many systems, such as ships, cranes, freighters and more, operate and produce great amounts of data. This is in fact the Internet of Things (IoT). These "things" range from ships and cranes to a single container. This data can be processed and analyzed with big data and AI tools. The insights from these processes improve and optimize the flow of products in the logistics value chain.

It should be noted that in recent years Israeli entrepreneurs are discovering the maritime field and the potential inherent in it as a 'vertical field' for technological developments, and there is already a fairly solid foundation for the expansion of this industry; however, complementary government activity is necessary for the development of the field. Among the commercial activities in the field of maritime technologies that already exist in Israel, the following should be noted:

Venture capital activity: theDOCK Maritime-Tech venture capital firm announced a second round of fundraising in the amount of 30 million dollars in 2022.[15] The Arieli Capital holding and investment company deals, among other things, with maritime technologies. The company operates the innovation center in Eilat (including activities in the field of aquaculture in the Negev) and also announced cooperation with the China Merchants Company, to manage an innovation center for maritime technology that will be established in China.[16]

The Beta site at Haifa Port: The port is working to establish projects in the field of technological innovation for the world of shipping, ports and logistics. However, it should be noted that due to the privatization processes of the port (the announcement of the winner of the privatization of the Haifa Port was made in August 2022, but the Israeli-

14 For a discussion on the topic, see Itai Sela, "Estimate of the Cost of Protecting the Sea Ports in Israel Against Cyber Threats", in Shaul Chorev and Ziv Rubinovitz (eds.), *Maritime Strategic Evaluation for Israel 2021/22* (Haifa: Maritime Policy & Strategy Research Center, University of Haifa, 2022), pp. 346–357.

15 theDock Company website: thedockinnovation.com.

16 Gonen, Overview of Blue Economy in Israel (Hebrew).

Indian consortium that won the tender has not yet started the actual operation),[17] activity regarding technological innovation has been hampered.[18]

The technological incubator at the Ashdod Port: Ashdod Port established an innovation incubator in the field of logistics, shipping and ports. Furthermore, the 500 Global accelerator, which specializes in managing technology incubators, joined the port's operations.[19]

Israeli National Center of Blue Economy: In July 2022, the National Center for Blue Economy was launched by the Municipality of Haifa. The center is managed by the municipal corporation HiCenter, which encourages the development of entrepreneurship in the city.[20]

Vessel production: there is one shipyard company in Israel intended for building ships. "Israel Shipyards" manufactures medium-sized vessels of up to 70 meters in size, such as Shaldag-class patrol boats or missile ships, mainly for military and law enforcement purposes (Coast Guard, etc.). These are shipyards with an international reputation in their niche of activity. Furthermore, unmanned military vessels were/are being produced by Rafael (the Protector ship), Elbit (Sigol), and IAI (Katina).

At the end of 2021, the Israel Aerospace Industries (IAI) signed a contract with the EDGE company from the United Arab Emirates for the joint production of autonomous vessels for a variety of military and commercial applications.[21] In the underwater field, ELTA (a subsidiary of IAI) has developed an unmanned submersible vessel with capabilities to replace sensors and tasks according to operational needs.[22]

Private companies: in the civil sector, a number of relatively large companies such as 'Totem Plus', which deals in navigation systems and is a leading company in the field of

---

17 "Gadot Won the Tender for the Privatization of the Haifa Port for NIS 4.1 Billion", *Calcalist*, July 14, 2022 (Hebrew).

18 "The Port of Haifa Publishes a Request for Tender for a Technological Innovation Project in the Field of Shipping", *port2port*, January 24, 2019 (Hebrew).

19 "Innovation at Ashdod Port", Ashdod Port, retrieved November 2022 (Hebrew).

20 The National Center for Blue Economy Website. blueeconomy-il.com.

21 Press Releases "EDGE Announces Strategic Deal with IAI to Develop Advanced Unmanned Surface Vessels" *IAI*, November 18, 2021.

22 Roy Nagler, "The Challenges in Operating Autonomous Vessels in the Era of Globalization – the Case of Autonomous Cargo Ships", in Shaul Chorev and Ehud Gonen (eds), *Maritime Strategic Evaluation for Israel 2019/20* (Haifa: Maritime Policy & Strategy Research Center, University of Haifa, 2020), 1–14.

maritime navigation systems and decision support systems, as well as the 'Orca', may be mentioned. The website of the Israeli Advanced Technologies Forum lists several dozen maritime companies, but this is only a partial list of the companies operating in Israel.[23] Zim is a large Israeli shipping company, but the company's core business is maritime and integrated transport and not technological developments. However, given the appropriate context, the fact that 'Zim' is an Israeli company may allow experimental installations of innovative technologies.

In addition to the maritime technology field being a potential catalyst for national growth, it can also encourage distinct growth in the Haifa Bay and the Western Galilee region. Since 2015, the government has been determining a social and economic development policy for the north of Israel and the city of Haifa. In the process, government decision No. 2262 was accepted in 2017 on the subject of 'Economic development of the northern district and complementary measures for the city of Haifa', which included a reference to the issue of the port and its infrastructure.[24] In 2020–2021, in accordance with a government decision on the 'development and advancement of Haifa Bay',[25] a committee of Director Generals from relevant government ministries was convened within the framework of the National Economic Council, and conducted a long and comprehensive procedure that focused mainly on the petrochemical industries in Haifa Bay, but encompassed all aspects of the economy and employment in the region. The committee determined the following:

> Analysis as part of the committee's work found that the relative advantages of the bay area include: knowledge-intensive industry, seaport and logistics, "green" production industries for energy and chemistry, and leisure tourism. Based on this analysis, there is great potential for employment in the Haifa Bay, and for the realization of the "Innovation Bay" plan.[26]

One of the committee's recommendations was the development of knowledge-intensive industrial areas in the Haifa region for the purpose of shifting the industrial focus of Haifa from the petrochemical industry to knowledge-intensive industries. This trend is in line with the Haifa Municipality's own policy for the development of the city as a center for knowledge-intensive industries. This policy is based on the fact that growth engines for the city are tourism, sea, aquaculture, environment, sustainability and security.

---

23 Maritime Technologies Forum website. israelmaritime.org

24 "Economic Development of the Northern District and Complementary Measures for the City of Haifa", Government Resolution No. 2262, January 8, 2017.

25 "Development and Advancement of Haifa Bay", Government Resolution No. 472, October 25, 2020 (Hebrew).

26 "Recommendations of the CEOs' Committee for the Development and Advancement of Haifa Bay", National Economic Council at the Prime Minister's Office, June 7, 2021 (Hebrew).

Advanced technologies in the field of shipping and ports can contribute to the economic development of the Israeli economy and growth within a sector in which hundreds of companies will operate, employing thousands of workers at high wages, and creating wide circles of employment and technological exchange, as is the case in the fields of space and unmanned aircraft and vehicles. There is a need to build an economic infrastructure that includes dedicated development plans for the field, beyond the activities of technology companies and private venture capital funds that already operate in this field, as well as the development of appropriate regulatory infrastructure, such as test and trials facilities.

The first step in this direction was the Ministry of Innovation, Science and Technology's statement regarding the sea as one of the five national priority areas. This decision must continue to be supported with an appropriate budget and regulatory activity, a process that is indeed taking place.[27]

Regional Cooperation Opportunities

Cross-border economic cooperation is one of the ways for building regional security stability, and this goes beyond the direct economic benefit inherent in them. The economic potential inherent in the joint project for each party drives a mutual desire to preserve the cross-border ventures despite upheaval and external events. Furthermore, direct channels of communication are opened between individuals and organizations on both sides of the border, which, in turn, also contribute to general stability. In the Israeli context, the QIZ project between Israel and Jordan and between Israel and Egypt,[28] as well as past collaborations between Israel and Egypt in the field of agriculture may be mentioned. Examples of these in recent years are cooperation in regard to gas fields, such as the agreement between Israel and Egypt and the establishment of a regional alliance in the eastern Mediterranean (see below). [29]

Technological collaborations with Cyprus and Egypt in the field of shipping technology and ports are unique, in light of the maritime characteristics of these countries (see below). It is possible to plan joint international experimental areas for shipping and logistic technologies, demonstration and feasibility testing facilities (beta site), international

---

27 The National Council for Civil Research and Development, "Bioconvergence, foodtech, Renewable Energies, Space and Blue-tech: these are the National Priority Areas for the State of Israel", the Ministry of Innovation, Science and Technology, September 4, 2022 (Hebrew).

28 Qualify Industrial Zones – QIZs are industrial zones in Jordan and Egypt where Israeli-owned or joint-owned factories benefit from duty-free exports of goods (mainly textiles) to the United States under the auspices of Israel's free trade agreement with the United States.

29 Danny Zaken, "It's official: Israel, the European Union and Egypt have signed a gas export agreement", *Globes*, June 15, 2022 (Hebrew).

cooperation to obtain funding from international organizations (such as the World Bank or European funds), to support joint projects and more.

Cyprus

Civil cooperation between Israel and Cyprus, especially in the areas close to the maritime domain, has a high potential for success. Being an island, Cyprus is dependent on the sea for every aspect of its existence. This island, with about one million inhabitants, has a world-class flourishing shipping industry, on a larger scale than that of Israel. The Cypriot fleet flying a national flag included (as of 2020) 1,056 ships with a total load of 35 million tons, in addition to many ships under flags of convenience or in partnership with Greek players (Greece is one of the most important shipping countries in the world).[30] Cyprus also supports entrepreneurship and innovation and tries to promote these fields. For example, with a chief scientist position, responsible for research and entrepreneurship.[31]

In recent years, diplomatic relations between Cyprus and Israel have been strengthened, especially in aspects of energy and maritime activity. The catalyst for this improved diplomatic relationship is common interests in energy issues such as gas and electricity on the one hand, and the existence of a common adversary – Turkey, on the other. Cyprus has been a member of the European Union since 2004. Israel and Cyprus have a common maritime border in the economic exclusive zones (EEZ) and thus, practically, Israel has a common maritime border with the European Union. The two countries agreed on the demarcation of their maritime border in an agreement signed in December 2010.[32] In 2021, the countries reached certain agreements regarding the Aphrodite-Yashi reservoir shared by both.[33] Israel and Cyprus also signed an agreement to connect the electricity grid between the countries with an underwater cable that will be the longest of its kind.[34]

---

30 "Maritime Profile: Cyprus", *UNCDATSTART, 2021.*

31 Cyprus's Chief Scientist for Research and Innovation Website. chiefscientist.gov.cy

32 Avi Bar-Eli, "Israel and Cyprus Agree on Economic Waters Border", *TheMarker*, December 19, 2010 (Hebrew).

33 "Minister Steinitz and his Counterpart from Cyprus – Natasa Pilides, Reach a Solution to the Dispute at the Aphrodite-Yashi Reservoir", Ministry of Energy, March 9, 2021 (Hebrew).

34 "Israel Connects to the European Electricity Grid: Minister Steinitz Signed a Memorandum for Laying the World's Longest Underwater Electricity Cable", Ministry of Energy, March 9, 2021 (Hebrew).

Egypt

In light of Israel's five wars with Egypt (1948, 1956, 1967, 1967-1970, 1973), a peace treaty signed in 1979 and Egypt's influence on what is happening in the Gaza Strip, the stability of relations with Egypt is a strategic goal.

Egypt is a key country in the field of global shipping, due to the Suez Canal that runs through its territory. About 10% of world trade is transported through the canal. The canal, which was expanded in recent years as part of an Egyptian national project, is operated by a government authority that runs hundreds of different vessels and employs thousands of workers. Port Said, at the northern exit of the canal, is one of the largest transshipment ports in the region.

A maritime border with Egypt has not been officially determined, and there is also the problem of defining a maritime domain for the Gaza Strip, located between the countries. However, at longer ranges in the EEZs, Israel and Egypt share a common maritime border, since there is an underwater gas pipeline between the countries. Economic cooperation in the field of blue economy, energy and shipping technologies between Israel and Egypt is also relevant in the Red Sea, where Egypt is in the midst of a great economic and maritime development boom.

The Israeli government decided on "a plan to promote and expand the economic ties between the State of Israel and the Arab Republic of Egypt".[35] This decision includes elements of joint development of a blue economy, in the fields of aquaculture (both in the Mediterranean and the Red Sea), energy from the sea, and marine tourism. Expansion of this program to the fields of shipping technology and logistics should also be considered.

The East Mediterranean Gas Forum

The East Mediterranean Gas Forum (EMGF) is a maritime economic cooperation forum for the countries of the Eastern Mediterranean. This forum began as the 'Hellenic Alliance' between Israel, Cyprus and Greece to which Egypt was also invited. Later, the framework was expanded into an established forum called the "East Mediterranean Gas Forum", which includes Greece, Israel, Jordan, Egypt, France, Cyprus and the Palestinian Authority. The United States and the European Union are observing members of the forum as well. Originally, the forum was established for the purpose of consultations on the construction

35 "A Plan to Promote and Expand the Economic Ties between the State of Israel and the Arab Republic of Egypt", Government Resolution No. 1522, Israel Government, May 29, 2022 (Hebrew).

of an underwater gas pipeline project that would centralize the export of gas from the economic waters of Israel, Cyprus and Egypt and reach the European markets via Italy.[36]

In addition to this, a 3+1 forum exists, including Israel, Cyprus and Greece as well as the United States. Within it, blue economy emerges as a relevant and important field to the relationship of the forum members.[37]

Strategic National Opportunities

On a strategic level, the development of maritime technologies will help to renew essential maritime knowledge that is gradually disappearing from Israel. it will also increase Israeli soft power, and provide diplomatic leverage for Israel in the international arena.

In Israel, there are six commercial ports (Haifa port, the Bay port, Ashdod port, the South port, Israel Shipyards and Eilat port) and three energy ports (Hadera, Ashkelon, Eilat). The cumulative length of the docks in these ports is more than 13.5 km and they use advanced technologies (the vast majority of which are not Israeli) such as semi-automatic bridge cranes, automatic facilities for bulk goods (grains and cement) and more. The ports are operated by Israeli governmental companies, alongside leading international companies such as SIPG from China, TIL from Switzerland and Adani from India.[38]

On the other hand, Israeli shipping is at a low. The fleet of ships owned and controlled by Israel stands at 35 ships alone (in 2021), of which only 7 ships raise the Israeli flag. The average age of merchant navy ships is 13.3. A total of 129 Israeli sailors are employed at the Israeli-owned and controlled merchant navy, all of them officers without ratings (qualified sailors).[39] These numbers are distinctly lower than those of the 'heyday' of Israeli shipping in the 1960s and 1970s, when dozens of ships sailed under the Israeli flag, with thousands of Israeli sailors.

The decline of Israeli shipping and the loss of knowledge and manpower in the maritime field, with only a few ships raising the Israeli flag, about a hundred Israeli naval officers and no Israeli ratings at all, has strategic effects on the country's international trade during emergencies, and it is likely (in view of past events) that global shipping will

---

36 "Cyprus, Greece, Israel and Italy Signed a Memorandum today in Nicosia for the Construction of the Gas Pipeline from Israel to Italy", Ministry of Energy, December 15, 2017 (Hebrew).

37 Israel's ambassador to Cyprus, Oren Anolik, on a Zoom call, June 2022.

38 In August 2022, the Adani Group from India won the tender to operate the Haifa Port but has not yet begun this operation.

39 *Shipping and Ports Statistical Yearbook 2021*, Administration of Shipping and Ports, Ministry of Transport, 2021, p. 101 (Hebrew).

avoid Israeli ports in such cases. Furthermore, the decline of Israel's commercial fleet means the loss of maritime knowledge essential to the management of Israel's ports and maritime domain. The development of maritime technologies is a tool for addressing Israel's maritime blindness, and to recognize, once again, the importance of the maritime domain to the Israeli public.

Technological leadership is a significant part of a country's soft power. The exchange of technology is often used as a currency in the diplomatic world. Countries with economic and technological power can exert more influence on other players in the international community in order to advance their goals. In the Israeli context, it is possible to see Israeli leadership in areas such as agriculture, water technology and energy, areas that promote Israel's position in the region and in the world, and allow it room for diplomatic maneuvering.

Global technological leadership allows leading countries to define international standards suitable for their local industry, thus leveraging leadership in a certain sector for further economic development which, in turn, preserves leading positions in that field.

Furthermore, exporting technologies enables the collection of much information that can be used by state or commercial companies in future developments and future economic impact. For example, the political power of a global social network platform – in light of the huge amount of information it contains – is immeasurably greater than the purely financial scope of the activity on it. Another example from the field of transportation is companies such as Boeing or Airbus in the aviation field, Maersk in the shipping field, major car manufacturers such as Toyota and more – all of these have much information regarding global trends that go far beyond the field of transportation in which they operate – this is due to the global aspects of these companies' activities. In light of the cross-sectional importance of the maritime trade, shipping and maritime security fields, a significant future technological presence in these fields also brings with it the ability to collect much information and with it a greater influence in the global arena.

Conclusions and Recommendations

It will probably be many more years before fully autonomous ships with no crew will sail the seas. However, it seems that we are in the midst of introducing advanced technologies to the field of shipping, and should certainly expect an increase in the level of vessel automation and the introduction of decision support systems, which will greatly lower the number of crew members on board the ships. Additionally, there may be ships that will be operated and supervised from the shore, where the crew will operate and

supervise several ships at the same time, or ships and smaller vessels without a crew that will sail on fixed and clear routes.

The development of maritime technologies is a catalyst for national growth, similarly to the fields of space, automobiles and aviation and can also be a major regional growth catalyst in the Haifa Bay area, as an alternative to the petrochemical industry. The development of maritime technologies can strengthen relations with Cyprus and Europe, as well as with Egypt, and can help Israel take a proper and respected place in the field of global shipping. Israel has a maritime heritage, but in recent decades maritime knowledge has been lost. This situation has strategic consequences, among other things, on the country's international trade during an emergency and the control of the Israeli maritime domain.

As in many fields, technology and legislation advance together, and the need for regulation that enables technological development, such as conducting sea trials in Israel on a regular basis as part of an infrastructure for the development of a blue economy, is increasing. This is in line with global trends in the development of blue economy, as well as the economic development trends in Israel, based on entrepreneurship and innovation.

Main Recommendations

1. Action must be taken to build a national plan to promote the field of maritime technologies. The announcement of an Israeli National Center of Blue Economy in Haifa, and the announcement of blue economy as a national priority by the Ministry of Innovation, Science and Technology are undoubtedly noteworthy progress, but these announcements must be broken down into practical plans and budgeted accordingly, and an appropriate regulatory framework must be promoted.
2. The maritime regulators must promote a regulation that allows experiments in advanced technologies for naval vessels, such as autonomous vessels.
3. On the issue of international standardization: the autonomous shipping trend is industry-driven, meaning it grows bottom up. Therefore, there is great significance to technological capabilities alongside standardization. It is recommended to act for the purpose of placing Israeli experts in the fields of technological standardization for the maritime domain, especially when it comes to maritime cyber. For this reason, together with the Standards Institution of Israel, it is recommended to integrate technical experts from Israel under ISO/TC 8 Ships and maritime technology committee, for activity in the next World Organization for Standardization teams.