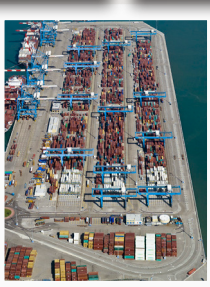
אוניברסיטת חיפה
University of Haifa
جامعة حيفا

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

MARITIME STRATEGIC EVALUATION FOR ISRAEL 2019/20

Chief editor: **Prof. Shaul Chorev**

Edited and produced by: **Ehud Gonen**



Components of national cyber security arrays in the civil maritime sector

Ofir Kafri[1]

This article presents examples of various methods used in cyber security arrays in the civil maritime sector in selected countries. In recent years, there has been progress in developing civil maritime cyber security arrays in a number of countries that have advanced in cyber security.[2] This trend has been reinforced, in part, by international and local cyber events and attacks.[3] Cyber security has even become part of the maritime strategies of some countries operating in the maritime domain.[4]

Different countries have established cyber security arrays in the maritime sector, with the goal of managing the risk to critical infrastructure and other facilities. These include, for example, maritime cybersecurity operations centers for ports and platforms for sharing information and facilitating coordination within the sector and with other sectors. Several countries are adopting cyber regulation that includes the maritime sector. Other related activity includes training and raising awareness, publishing directives, introducing standards, creating R&D infrastructure and fostering international cooperation.

Due to the limited scope of the article, it presents only some of the maritime cyber security array methods applied in the selected countries: Singapore, the Netherlands, Canada, Denmark and the United States. These countries were selected because they

1 This chapter is part of a study written with the assistance of a research grant from the Center for Cyber, Law and Policy (CCLP) and the Maritime Policy and Strategy Research Center (HMS).

2 International Telecommunication Union (ITU), Global Cybersecurity Index (GCI) 2018: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

3 Cyber events have occurred in ships, offshore drilling rigs, commercial port infrastructure, energy terminals (oil and gas), shipping companies, freight forwarding company, port service providers, shipping agencies, maritime regulators and others. See, for example: United States Senate, Report of United States Senate Committee on Armed Services, inquiry into cyber intrusions affecting U.S. transportation command contractors, iii, 2014; Coast Guard Maritime Commons site, Lt. Jodie Knox, Coast Guard Commandant on Cyber in the maritime domain, June 15, 2015; The Columbian, Dameon Pesanti, Port of Vancouver meeting hindered by cyberattack, March 10, 2017; The New York Times site, Thomas Erdbrink, Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet, published April 23, 2012; Clarkson PLC Annual Report 2017, Page 19, 83; Danish Broadcasting Corporation news site, Michael Lund and Niels Fastrup, Fremmed stat spionerede mod dansk ministerium (Foreign State spied on Danish ministry), published September 21, 2014.

4 See, for example, maritime strategy documents of the US and France: U.S. Navy, Marine Corps, and Coast Guard, A Cooperative Strategy for 21ST Century Seapower, March 2015, page 33-34; France National strategy for the security of maritime areas, October 2015, page 23-24.

play an important role in the global maritime sector and/or because they are developing national maritime cyber arrays. It should be noted that the capability, operational quality and efficiency of the arrays differ from one country to the next. The article concludes by outlining the main components in existing cyber arrays; these components are also recommended by international guides on cyber security.

Singapore's maritime sector

The civilian maritime sector is an important component in Singapore's economy and accounted for 7 percent of the country's GDP in 2017 and about 170,000 jobs.[5] Singapore is located in the Straits of Malacca and Singapore (SOMS), a critical strategic route in the global maritime transportation system. Every year, almost half of all global commercial maritime cargo and about 70 percent of Asia's oil imports pass through these two straits.[6] The Port of Singapore ranks second in the world in container traffic.[7] The cyber strategy of Singapore stresses the importance of defending maritime activity.[8] The Cyber Security Agency of Singapore (CSA) works with the Maritime and Port Authority (MPA) of Singapore to protect the civilian maritime sector.

The Maritime Cybersecurity Operations Center (MSOC) in Singapore began operations in May 2019, monitoring and coordinating all of the critical information infrastructure in the maritime sector.[9] The MSOC enables the MPA to work with critical information infrastructure operators to investigate cyber threats and events in the maritime sector. Plans call for connecting the MSOC to the MPA's Port Operations Control Centre (POCC), with the goal of facilitating a rapid and comprehensive response to cyber events.[10]

---

5 Singapore Ministry of Trade and Industry, Enterprise Singapore, Industry Profile, 2018: https://www.enterprisesg.gov.sg/industries/type/sea-transport/industry-profile

6 Singapore Ministry of Defence, Fact Sheet: The Malacca Straits Patrol, 21 Apr 2015: https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2016/april/2016apr21-news-releases-00134

7 Lloyds list, One Hundred Ports 2019: https://lloydslist.maritimeintelligence.informa.com/one-hundred-container-ports-2019

8 Singapore's Cybersecurity Strategy, Cyber Security Agency of Singapore, 10 Oct 2016: https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf

9 Cyber Security Agency of Singapore, Singapore's Operational Technology Cybersecurity Masterplan 2019, 01 Oct 2019, page 41: https://www.csa.gov.sg/~/media/csa/documents/publications/ot_masterplan/csa_ot_masterplan.pdf

10 Singapore Computer Emergency Response Team (SingCERT), Maritime, 08 Oct 2019: https://www.csa.gov.sg/singcert/publications/maritime

With respect to the training of personnel in cyber security, a new and more comprehensive course is being developed in cooperation with the Singapore Shipping Association and the Singapore Polytechnic. The course is designed to train personnel in cyber risk management, cyber security counter-measures and other subjects.[11] In addition, Singapore is conducting activities aimed at raising awareness of maritime cyber security, including seminars for both the private and public sectors.[12]

The Cybersecurity Act that went into effect in 2018 provides broad powers to the Commissioner of Cybersecurity and other officials appointed by the commissioner or by the relevant minister. The delegated powers facilitate the gathering and sharing of information, investigation and more. The law establishes cyber security requirements for essential infrastructure in the maritime sector. This includes infrastructure for monitoring and managing shipping, the operation of various types of terminals, refueling infrastructure, rescue operations and more.[13]

The Maritime Cybersecurity Research Program, which focuses on the protection of shipboard systems, will be carried out through cooperation between the MPA, institutions of higher education in Singapore and the Singapore Maritime Institute (SMI).[14]

International collaboration between Singapore and other countries also includes the sharing of professional information on the protection of infrastructure. For example, a memorandum on cyber security cooperation was signed with the Netherlands in 2016.[15] Another example is the hosting of an international forum for safety of navigation and environmental protection in the Singapore and Malacca Straits, which also addresses

11 Maritime and Port Authority of Singapore, New 24/7 Maritime Cybersecurity Operations Centre to Boost Cyber Defence Readiness, 16 May 2019: https://www.mpa.gov.sg/web/portal/home/media-centre/news-releases/detail/8a5114cf-8214-4b46-8999-2c6c42433b1e

12 Maritime and Port Authority of Singapore, Shaping the Future of a Cyber-smart Maritime Industry, 24 April 2018: https://www.mpa.gov.sg/web/portal/home/media-centre/news-releases/detail/0c373e30-7ff8-4a8a-a1d8-32bd3299ea4d

13 Singapore Legislation Division of Attorney-General's Chambers, Cybersecurity Act 2018, 12 Mar 2018: https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312; Cyber Security Agency of Singapore, Cybersecurity Act, Explanatory Statement: https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/cybersecurity%20act%20-%20explanatory%20statement.pdf

14 Singapore Maritime Institute, About us: https://www.maritimeinstitute.sg/about-us; Maritime and Port Authority of Singapore, New 24/7 Maritime Cybersecurity Operations Centre to Boost Cyber Defence Readiness, 16.5.2019.

15 Singapore and the Netherlands to Strengthen Cyber Security Cooperation, Cyber Security Agency of Singapore, 12 Jul 2016: https://www.csa.gov.sg/news/press-releases/csa-signs-mou-with-the-netherlands-to-strengthen-cyber-security-cooperation

cyber security.[16] The MPA is planning to establish international cooperation between parallel authorities with the goal of sharing information on threats and cyber events.[17]

The maritime sector was included in national cyber exercises managed by the Cyber Security Agency of Singapore in 2017 and 2019. The exercises tested the resilience of the maritime sector in a variety of cyber scenarios. The simulations included other critical sectors, with the goal of testing the preparedness for major cyber events, including inter-sectoral cooperation.[18]

The maritime sector in the Netherlands – the Rotterdam and Amsterdam ports

The Netherlands' Network and Information Systems Security Act, pursuant to the European Union's NIS Directive (EU) 2016/1148, went into effect in 2018.[19] The law requires providers of an essential service, including those in the maritime sector, to meet cyber security requirements. It authorizes government ministries or the national Computer Security Incident Response Team (CSIRT), according to the circumstances, to require reporting on cyber events. Additional delegated powers relate to investigation, auditing, sanctions, etc.[20]

The **Port of Rotterdam** is ranked first in Europe in volume of container traffic and eleventh in the world.[21] The port is an important component in the Netherlands' economy and in Europe's commercial maritime traffic.[22] In 2017, almost half of the commercial traffic in

16 Maritime and Port Authority of Singapore, 8th Co-operation Forum addresses key issues relating to Straits of Malacca and Singapore, October 2015: https://www.mpa.gov.sg/web/portal/home/media-centre/news-releases/detail/c8c677d0-07d1-4d9c-b634-ac416c4c29e9; Co-operative Mechanism on Safety of Navigation and Environmental Protection in the Straits of Malacca and Singapore, October 2015: https://www.soefartsstyrelsen.dk/Presse/Nyheder/Documents/Program_Co-operative%20Forum_Singapore.pdf

17 Maritime and Port Authority of Singapore, New 24/7 Maritime Cybersecurity Operations Centre to Boost Cyber Defence Readiness, 16.5.2019.

18 Cyber Security Agency of Singapore site, 11 CII Sectors Tested on More Complex Cyber Attack Scenarios, 04 Sep 2019: https://www.csa.gov.sg/news/press-releases/exercise-cyber-star-2019

19 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

20 Netherland Network and Information Systems Security Act (Wet beveiliging netwerk- en informatiesystemen), Act of 17 October 2018: https://wetten.overheid.nl/BWBR0041515/2019-01-01#Hoofdstuk4_Paragraaf1_Artikel5

21 World shipping Council, Top 50 World Container Ports: http://www.worldshipping.org/about-the-industry/global-trade/top-50-world-container-ports

22 Erasmus University Rotterdam, Centre for Urban, Port and Transport Economics, The Rotterdam effect, 18 Dec 2018: https://www.eur.nl/en/upt/news/rotterdam-effect; W. Heijman et al, The impact of world trade on the Port of Rotterdam and the wider region of Rotterdam-Rijnmond, Case Studies on Transport Policy, 5 (2017) 351–354.

the port (by cargo weight) served Europe and about one quarter served Asia.[23] A law enacted in 2018 defines the port as a provider of an essential service, thus obligating it to fulfill a number of cyber security requirements.[24]

The port operates in cooperation with the country's National Cyber Security Center (NCSC). Several cyber security bodies have been created at the port. One example is a cyber notification desk that receives reports of major cyber events; the desk has been operating as part of the port's operations center since 2018. Companies operating in the port that are subject to the ISPS code[25] or EU regulations[26] are required to report major cyber events to the notification desk and in some cases to other entities as well. These events relate to situations that affect the security of traffic in the port, the entry and exit of ships, and the implementation of the port security plan.[27]

In 2016, a port cyber resilience officer was appointed and a plan of action was formulated. The officer's area of responsibility includes training, raising awareness and managing cyber risks. To this end, committees were established to deal with the various aspects of cyber security, such as legislation and exercises. The cyber resilience officer works in cooperation with law enforcement agencies, municipal authorities and other bodies.[28] The port carries out cyber exercises and maintains a staff of cyber security experts who are responsible for protecting the port infrastructure.

23 Port of Rotterdam Authority, Facts and Figures, 2019: https://www.portofrotterdam.com/sites/default/files/facts-and-figures-port-of-rotterdam.pdf

24 Netherland Network and Information Systems Security Act (Wet beveiliging netwerk- en informatiesystemen), Act of 17 October 2018; Decision on network and information security (Besluit beveiliging netwerk- en informatiesystemen), Decree of 30 October 2018: https://wetten.overheid.nl/BWBR0041520/2019-01-01

25 International Ship and Port Facility Security (ISPS) is part of the Safety of Life At Sea Convention (SOLAS). The goal of the code is to strengthen the security of shipping and port facilities. For further information, see: International Maritime Organization (IMO), SOLAS XI-2 and the ISPS Code: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

26 Regulation (EC) no. 725/2004; Netherland Port Security Act: https://wetten.overheid.nl/BWBR0016991/2010-10-01

27 Port of Rotterdam, policy document port cyber notification desk: https://www.portofrotterdam.com/sites/default/files/policy-document-port-cyber-notification-desk.pdf?token=waAgc_VH; Port Cyber Hotline operational, 11 June 2018: https://www.portofrotterdam.com/en/news-and-press-releases/port-cyber-hotline-operational

28 Port of Rotterdam site, Port of Rotterdam appoints Port Cyber Resilience Officer, 13 June 2016: https://www.portofrotterdam.com/en/news-and-press-releases/port-of-rotterdam-appoints-port-cyber-resilience-officer

Cyber security conferences have been held to raise awareness and improve cyber training for businesses that operate in the port. The port offers a program of cyber security assistance for small businesses, which includes online training and tools that help to identify cyber weaknesses. The assistance is based on the realization that small businesses are important to the port's activity and are connected to important port systems, but do not have the resources to deal with complex cyber issues and therefore may constitute a weak link.[29]

The **Port of Amsterdam** initiated a program to upgrade cyber security in 2018. It presented e-learning modules about information security with the aim of raising awareness of the issue among workers and other stakeholders. The port recruited an information security officer and established a cyber security hotline.[30] The hotline receives voluntary reports in addition to compulsory reports from entities that are subject to the ISPS code.

The Port of Amsterdam cooperates in this area with the NCSC, the Port of Rotterdam, the Digital Trust Center (DTC) and other entities. In addition, the port has initiated a program for sharing information with the private and public sectors, including law enforcement agencies. It also sponsors public information events in cyber security in order to raise awareness and to provide professional information.[31]

Canada's maritime sector

A government forum called the Maritime Cyber Risk Project constitutes the basis for cooperation between ten different bodies from various ministries. The forum's goal is to propose possible solutions to cyber threats in the maritime sector.[32]

The Canadian Cyber Incident Response Center (CCIRC) operates a digital platform for disseminating information to critical infrastructure sectors and for enhancing cooperation. The platform facilitates the distribution of information according to levels

29 Port of Rotterdam site, How the Port of Rotterdam is investing in cybersecurity, 06 December 2016: https://www.portofrotterdam.com/en/news-and-press-releases/how-the-port-of-rotterdam-is-investing-in-cybersecurity

30 Port of Amsterdam Annual Report 2018, page 67, 72-73. Published on 6 May 2019: https://jaarverslag2018.portofamsterdam.com/wp-content/uploads/2019/06/Port-of-Amsterdam-Annual-Report-2018_final.pdf

31 Port of Amsterdam, Cyber security in the North Sea Canal Area (NSCA): https://www.portofamsterdam.com/en/port-amsterdam/organisation/cyber-security-nsca

32 NATO Association of Canada, Canada's Cyber Security: A Discussion with Public Safety Canada, 22 August 2018: http://natoassociation.ca/canadas-cyber-security-a-discussion-with-public-safety-canada

of security classification. The CCIRC is available to assist in the management of cyber events in critical infrastructure, including in the maritime sector, and operates support programs to help entities in the private sector carry out risk assessments.[33]

Entities subject to the maritime security regulations are required to include cyber security in their assessment and security programs. In certain cases, there is a requirement to report a cyber event to government bodies.[34]

Transport Canada, a federal institution, is responsible for establishing a cooperative network for conducting a sectoral risk assessment on an annual basis.[35] In 2016, Transport Canada published a document on cyber security best practices for the maritime sector.[36] Similar documents were published in 2016-2017 for the maritime sector in the United Kingdom. The documents present recommended methods for cyber security in port infrastructure and shipping.[37] France also published a series of documents in 2016-2018 on maritime cyber security[38] and, in 2019, the European Union Agency for Cybersecurity (ENISA) published best practices for cybersecurity in ports.[39]

33 Public Safety Canada, Fundamentals of Cyber Security for Canada's CI Community, Date modified: 2019-01-21: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx

34 Transport Canada, Marine Security Operations Bulletin, No: 2014- 001: https://www.tc.gc.ca/media/documents/marinesecurity/MSOB_BSOM_2014-001-en.pdf

35 Canada Action Plan for Critical Infrastructure, Date modified: 2018-01-31: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr/index-en.aspx#aB

36 Transport Canada, Understanding Cyber Risk: Best Practices for Canada's Maritime Sector Page 16-17: http://publications.gc.ca/collections/collection_2016/tc/T86-21-2016-eng.pdf

37 UK Department for Transport & Institution of Engineering and Technology, Ports and port systems: cyber security code of practice, 16 August 2016: https://www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice; Ship security: cyber security code of practice, 2017: https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice

38 France Ministry of Environment, Energy and The Sea, Directorate-General for Infrastructure, Transport and the sea, Maritime Affairs Directorate, Cyber Security - Assessment and Protection of Ships, September 2016 Edition: https://www.ecologique-solidaire.gouv.fr/sites/default/files/Guideline%201%20-%20Cyber%20security%20-%20Assessment%20and%20protection%20of%20ship.pdf; Cyber Security – Reinforcing the Protection of Industrial Systems on a Ship, France Directorate-General for Infrastructure, Transport and the sea, Maritime Affairs Directorate, January 2017 Edition

39 European Union Agency for Cybersecurity (ENISA), Port Cybersecurity - Good practices for cybersecurity in the maritime sector, November 26, 2019: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector/at_download/fullReport. For more examples of cyber security good practices in the maritime sector please see: BIMCO, The Guidelines on Cyber Security Onboard Ships, Version 3: https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/cyber-security-guidelines-2018.ashx

Canada's Marine Security Operations Centers are responsible for managing events in the maritime domain. The centers assist in the assessment of risk to ports, vessels and maritime facilities. Each year, about 7,000 risks assessments are carried out for vessels entering Canada's maritime domain.[40]

The centers bring together various governmental bodies involved in the maritime domain. The centers focus on identifying and reporting maritime activity that poses a potential threat to security and safety.[41] In recent years, the area of cyber security has been added to the centers' responsibilities.

Denmark – Implementation of a maritime cyber security strategy

Denmark's national cyber strategy cites the maritime sector as one of the country's critical infrastructures. A cyber strategy document that specifically addresses the maritime sector was published in January 2019 and some of its recommendations have already been implemented.[42] The largest container shipping company in the world—A.P. Moller-Maersk—is headquartered in Denmark. A major cyber attack against Maersk in 2017 harmed the company and disrupted port operations in a number of countries.[43]

The Centre for Cyber Security (CFCS) provides assistance to the Danish Maritime Authority (DMA). The cyber strategy document states that the DMA should serve as a liaison between the maritime sector and the CFCS. Cooperation between the bodies includes the analysis and sharing of information on threats and assistance in risk evaluations for the maritime sector.[44] The first assessment was released to the public in 2017 and included recommendations for cyber security.[45]

---

40 Transport Canada, Transport Canada defends Canada's waterways and coastlines, 2019-03-07: https://www.tc.gc.ca/eng/transport-canada-defends-waterways-coastlines.html

41 Government of Canada, Marine Security Operation Centres, 2013-05-23: https://www.tc.gc.ca/eng/marinesecurity/operations-269.html; Canadian Coast Guard site, 2017-12-14: http://www.ccg-gcc.gc.ca/eng/CCG/Maritime-Security/MSOC

42 Danish Ministry of Finance, Danish Cyber and Information Security Strategy 2018-2021, Page 8, 40: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf; Danish Maritime Authority, Cyber and Information Security Strategy for the Maritime Sector: https://www.dma.dk/Documents/Publikationer/Cyber%20and%20Information%20Security%20Strategy%20for%20the%20Maritime%20Sector.pdf

43 MAERSK Site, News Release, A.P. Møller - Mærsk A/S Cyber attack update, June 28, 2017: http://investor.maersk.com/node/19831/pdf

44 DMA, Cyber and Information Security Strategy for the Maritime Sector, page 8-9.

45 Denmark Threat Assessment Branch under the Centre for Cyber Security, The cyber threat against the maritime sector, March 2017: https://fe-ddis.dk/cfcs/CFCSDocuments/The_Cyber_Threat_to_the_Maritime_Sector_march.pdf

In June 2018, a maritime cybersecurity unit was established in the DMA. The unit is responsible for implementing the measures prescribed in the strategy document, and serves as an advisory body, a communication center for the maritime sector and a source of expertise in the DMA. The unit is also responsible for coordinating an action plan with the maritime sector in areas such as regulation, training and raising awareness.[46] It participates in a cyber forum that includes all of the cyber units in Denmark's critical sectors. The goal of the forum, which operates in partnership with the CFCS, is to share information on threats and cyber events, and to promote cooperation between the various sectors.[47]

The DMA published an order on maritime cyber security that went into effect in February 2019. The order implements part of the European Union's NIS directive on cyber security (Directive (EU) 2016/1148)[48] and includes a number of obligations that apply to DMA-appointed operators of a maritime service. For example, in certain cases, there is an obligation to report a cyber event to the DMA and to the CFCS. Another requirement is to become certified as meeting international cyber security standards within two years of receiving an appointment from the DMA.[49]

The DMA works to foster cooperation in the cyber security field with other countries.[50] A cyber security forum that includes all of the authorities that have any direct influence on the maritime sector in Denmark is slated to be inaugurated in 2020-2021. The forum will prepare plans for responding to cyber events and emergencies, coordinate cyber exercises in the sector and more.[51]

---

46 Danish Maritime Authority, Danish Maritime Cybersecurity Unit: https://www.dma.dk/SikkerhedTilSoes/Cybersikkerhed/Sider/default.aspx

47 Center for Cyber Security, De samfundskritiske sektorer og CFCS drøfter hændelseshåndtering og varsler: https://fe-ddis.dk/cfcs/nyheder/arkiv/2019/Pages/tredje-moede-i-vidensdelingsnetvaerket.aspx

48 New maritime regulation supports prevention of cyber attacks, Danish Maritime Authority, 31 January 2019: https://www.dma.dk/Presse/Nyheder/Sider/New-maritime-regulation-prevention-of-cyber-attacks.aspx

49 Danish Maritime Authority, Order no. 46 of 15 January 2019, Order on the security of network and information systems of importance to the safety and navigation of ships: https://www.dma.dk/Vaekst/Rammevilkaar/Legislation/Orders/Order%20on%20the%20security%20of%20network%20and%20information%20systems%20of%20importance%20to%20the%20safety%20and%20navigation%20of%20ships.pdf

50 DMA, Cyber and Information Security Strategy for the Maritime Sector, page 6-7

51 Ibid, page 9-10.

The United States – The maritime sector and the Port of Los Angeles

The U.S. Coast Guard, which is responsible for cyber security in the American maritime sector, published its strategy for cyber security in 2015.[52] There is extensive regulation of maritime security in the U.S.[53] Under certain conditions specified in the regulations, there is an obligation to report a cyber event to the Coast Guard, which operates the National Response Center (NRC) that deals with these reports.[54] The Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) provides assistance to critical infrastructure. This includes transportation infrastructure, which encompasses the maritime sector.[55] The NCCIC operates a Hunt and Incident Response Team (HIRT) to assist organizations that have been attacked and request its intervention.[56] In addition, the Maritime and Port Security Information Sharing and Analysis Organization (MPS-ISAO), a non-profit partnership of the private and public sectors, serves as a platform for sharing information in the maritime sector.[57]

The Port of Los Angeles, ranked first in container traffic in the U.S., operates the Cyber Security Operations Center (CSOC). The CSOC is responsible for port infrastructure and is considered the first of its kind in the country. The port reported in 2019 that it is

52 Maritime Transportation Security Act of 2002, Executive Order 13636, Presidential Policy Directive 21, the Department of Homeland Security Blueprint for a Secure Cyber Future (2011), the 2014 DHS Quadrennial Homeland Security Review, the National Infrastructure Protection Plan of 2013, and the Department of Defense Cyber Strategy of 2015.

53 Maritime Transportation Security Act of 2002, 107th Congress, PUBLIC LAW 107–295—NOV. 25, 2002: https://www.congress.gov/107/plaws/publ295/PLAW-107publ295.pdf; Electronic Code of Federal Regulations (e-CFR) Title 33. Navigation and Navigable Waters Chapter I. Coast Guard, Department of Homeland Security, Subchapter H. Maritime Security Part 104-106. Vessels: Shttps://www.law.cornell.edu/cfr/text/33/part-104

54 Title 33 Code of Federal Regulations (CFR) §101.305 – Reporting, page 341-342: https://www.govinfo.gov/content/pkg/CFR-2015-title33-vol1/pdf/CFR-2015-title33-vol1-sec101-305.pdf; U.S. Coast Guard, Marine Safety Information Bulletin, Cyber Adversaries Targeting Commercial Vessels, May 24, 2019.

55 U.S DHS, National Cybersecurity and Communications Integration Center: https://www.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_NCCIC%20ICS_S508C.pdf

56 Marine Safety Alert, Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels, July 8, 2019: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf

57 U.S Coast Guard, The Maritime and Port Security Information Sharing & Analysis Center: https://homeport.uscg.mil/Lists/Content/DispForm.aspx?ID=45422&Source=/Lists/Content/DispForm.aspx?ID=45422; MPS-ISAO site: https://mpsisao.org

the only one in the country that is certified as meeting the cyber standard ISO 27001.[58] A plan to establish a Cyber Resilience Center to serve all of the entities connected to the port was initiated in 2019. The new center is expected to serve as a platform for sharing information and professional knowledge, coordinating operations and more.[59]

Conclusion and recommendations

This article highlights several key components in national cyber security arrays in the civilian maritime sector. The following summary of these components is not an exhaustive list of all possibilities. There are variations that can be tailored to the specific conditions and characteristics of each country. Wise use of the various tools, while establishing an optimal cyber security structure in the maritime sector, can support the effective management of the cyber domain.

A number of international guides offer professional insights that can assist in the creation of sectoral cyber security arrays. The arrays presented in this article make use of tools that are generally similar to those presented in the guides. The NATO Cooperative Cyber Defense Centre of Excellence (NATO CCDCOE), the European Union Agency for Cybersecurity (ENISA) and the International Telecommunications Union (ITU) are among the organizations that have published such guides.[60]

Here is a list of recommended components of a national cyber security array in the civilian maritime sector. These components are used in arrays worldwide and presented in the leading international cyber security guides:

Structure of the arrays: Main bodies and entities

1. **A national multi-sector cyber security body** – Serves as a professional resource for assisting the entity responsible for cyber security in the maritime sector. This body provides professional information, guidance, management of multi-sector exercises, a platform for cross-sectoral cooperation, etc.

---

58 Port of Los Angeles, Port Proposes the Creation of a Cyber Resilience Center with Stakeholders, April 25, 2019: https://www.portoflosangeles.org/references/news_042519_cybersecurity

59 Port of Los Angeles Cyber Resilience Center, Request for Proposals, July 24, 2019: https://kentico.portoflosangeles.org/getmedia/5d304eb8-71cf-4ba5-992c-86e311b5a682/RFP-Port-of-Los-Angeles-Cyber-Resilience-Center

60 NATO Cooperative Cyber Defense Centre of Excellence, National Cyber Security Strategy Guidelines, 2013: https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf; European Union Agency for Cybersecurity, NCSS Good Practice Guide, November 14, 2016: https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport; International Telecommunication Union (ITU), Guide to Developing a National Cybersecurity Strategy, 2018: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

2. **A maritime cyber security body** – Usually operates within a government entity responsible for the civilian maritime sector. This body interacts with the various entities in the maritime sector. Its functions may include implementation of programs for training and raising awareness, management of exercises in the sector, assistance and consultation, assessment of sectoral risks and threats, publishing of directives, etc. In addition, a cyber security operations center that operates in the maritime sector can facilitate the ongoing management and rapid response to any cyber activity in the sector. The center can provide a full picture of what is happening in the sector, can coordinate the information received from the various sources, can manage the response to major cyber events, etc.
3. **Cyber security entities in essential and non-essential maritime infrastructure** – Ports and maritime facilities should have a cyber security officer and a cyber security team if necessary. There is also an option to establish a cyber desk, a cyber security operations center, etc.

Training and awareness-raising programs

Training and awareness-raising programs among various audiences, such as workers in government entities connected to the maritime sector, workers at essential infrastructure and any others active in the maritime sector. The programs are usually tailored to each group.

Risk assessment

Risk assessment for the maritime sector, specific infrastructure and facilities, etc.

Exercises in the maritime sector and in a multi-sectoral framework

1. Participation of the sectoral cyber body and/or essential infrastructure participants in national cross-sectoral exercises.
2. Exercises in the maritime sector, including a number of entities or the entire sector.
3. Exercises at infrastructure facilities and in specific bodies.

Cooperation programs: Coordination, planning, guidance and sharing of information

1. **A multi-sectoral forum** – Participation in a national cross-sectoral forum for coordination and cooperation, including representatives of the body responsible for the maritime sector.
2. **Forum of government entities and/or essential entities** – Forum for coordination and cooperation that brings together all government bodies and critical infrastructure in the maritime sector. In some cases, the creation of a government forum that

includes only the governmental entities connected to maritime cyber security is recommended.

3. **Forum for all stakeholders in the civilian maritime sector** – A forum for coordinating and sharing information and capabilities, bringing together all of the entities in the maritime sector.

International cooperation

Cooperation with other countries, private and public bodies and international institutions in areas such as research, training, coordination of activity, intelligence, etc.

Research programs

A research program that includes academia, the government and the private and public sectors in the areas of cyber security in the maritime sector.

Regulation that provides means of enforcement, capabilities and tools

Legislation that provides efficient tools for managing cyber security in the maritime sector, while creating appropriate checks and balances. The legislation can include a legal foundation for establishing cyber bodies in the array. In addition, it can specify obligations such as the duty to report defined cyber events to the relevant government bodies. It is also recommended to establish a cyber entity with powers for gathering information, issuing directives and/or standards, supervision and oversight, investigation and management of cyber events in certain cases, etc.

Continuity and recovery plans

Preparing and implementing continuity and recovery plans for the maritime sector in general, and specifically for bodies and infrastructure in the maritime sector.