**Components of national cyber security arrays in the civil maritime sector**

**Ofir Kafri[[1]](#footnote-1)**

This article presents examples of various methods used and implemented in cyber security arrays in the civil maritime sector in some selected countries. In recent years, there has been progress in the development of civil maritime cyber security arrays in some of the countries that are advanced in cyber security.[[2]](#footnote-2) Cyber events and attacks in the maritime domain that have had international and local effects, as well as other factors, have led to the reinforcement of this trend.[[3]](#footnote-3) Cyber security has even become part of the maritime strategies of some countries that operate in the maritime domain.[[4]](#footnote-4)

Countries have established cyber security arrays in the maritime sector, which include a variety of methods, with the goal of managing the risk to critical infrastructures and other facilities in the sector. These include, for example, maritime cybersecurity Operations centers for ports and platforms for the sharing of information and coordination within the sector and with other sectors. Cyber regulation that includes the maritime sector is being adopted in several countries. Other examples include training and raising awareness programs, publishing of directives and the introduction of standards, the creation of Research and development infrastructure, international cooperation, etc.

The scope of the article makes is possible to present only some of the maritime cyber security arrays methods installed in the selected countries presented in this article, namely the Singapore, Netherlands, Canada, Denmark, United States. These countries were selected for being Important factors in the global maritime sector and/or because they are developing national maritime cyber arrays. It should be mentioned that there are differences with respect to capability, operational quality and efficiency of components of the arrays between the various countries. The conclusion will present the main components in existing cyber arrays that are also recommended by international cyber security guides.

**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]](#footnote-5) Singapore is located in the Strait of Malacca and Singapore (SOMS) which is considered to be a critical strategic route within the global maritime transportation system. Every year, almost one-half of all global commercial maritime cargo and about 70 percent of Asia’s oil imports pass through these two straits.[[6]](#footnote-6) Singapore Port ranks second in the world in terms of container traffic.[[7]](#footnote-7) The cyber strategy of Singapore stresses the importance of defending maritime activity.[[8]](#footnote-8) The Cyber Security Agency of Singapore (CSA) is working with the Maritime and Port Authority (MPA) of Singapore to protect the civilian maritime sector.

The Maritime Cybersecurity Operations Center in Singapore began operations in May 2019. The Center monitors and coordinates all of the critical information infrastructures in the maritime sector.[[9]](#footnote-9) The Center is meant to allow the MPA to work with critical information infrastructure operators in order to investigate cyber threats and events in the maritime sector. The Cyber Center will be connected to the Port Operations Control Centre (POCC) of the MPA, with the goal of facilitating a rapid and comprehensive response to cyber events.[[10]](#footnote-10)

With respect to the training of personnel in cyber security, a new and more comprehensive course is being developed. The course is being developed in cooperation with the Singapore Shipping Association and the Singapore Polytechnic and is designed to train personnel in, among other things, the management of cyber risk and cyber security counter-measures.[[11]](#footnote-11) In addition, there are activities that are aimed at raising awareness of maritime cyber security, such as seminars that include both the private and public sectors.[[12]](#footnote-12)

The new cyber law that went into effect in March 2018 provides broad powers to the Commissioner of Cybersecurity and other officials who will be appointed by him or by the relevant minister. The delegated powers facilitate the gathering of information, investigation, sharing of information, among other things. The law establishes requirements with regard to cyber security of infrastructures in the maritime sector that have been defined as essential, such as monitoring and management of shipping, operation of various types of terminals, refueling infrastructure, rescue operations, etc.[[13]](#footnote-13)

The maritime cyber 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]](#footnote-14)

There is international cooperation between Singapore and other countries which includes the sharing of professional information on the protection of infrastructures. For example, in 2016 a memorandum on cyber security cooperation was signed with Netherlands.[[15]](#footnote-15) Another example is the hosting of an international forum for Safety of Navigation and environmental protection in the Singapore and Malacca Straits, which includes cyber security.[[16]](#footnote-16) The MPA is planning to establish international cooperation between parallel authorities with the goal of sharing information on threats and cyber events.[[17]](#footnote-17)

National cyber exercises that are managed by the Cyber Security Agency of Singapore included the maritime sector in 2017 and 2019. The exercises tested the resilience of the maritime sector to a variety of cyber scenarios, among others. The simulations included other critical sectors, with the goal of testing the preparedness for major cyber events, including inter-sectoral cooperation.[[18]](#footnote-18)

**The maritime sector in Netherland – the Rotterdam and Amsterdam ports**

The Netherland Network and Information Systems Security Act went into effect in 2018 and it relates to the EU NIS directive (Directive (EU) 2016/1148).[[19]](#footnote-19) The law requires providers of an essential service, including those in the maritime sector, to meet cyber security requirements. It delegates power to the government ministries as set out in the law or to 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]](#footnote-20)

The **port of Rotterdam** is ranked first in Europe with respect to volume of container traffic and eleventh in the world.[[21]](#footnote-21) The port is an important component in Netherland’s economy and in Europe’s commercial maritime traffic.[[22]](#footnote-22) In 2017, almost half, by cargo weight, of the commercial traffic in the port served Europe and about one-quarter served Asia.[[23]](#footnote-23) The port is defined as provider of an essential service according to a 2018 law and as a result it is obligated to fulfill a number of cyber security requirements..[[24]](#footnote-24)

The port operates in cooperation with the National Cyber Security Center (NCSC). A number of cyber security bodies have been created in the port. One example is a cyber notification desk that receives reports of major cyber events day and which 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]](#footnote-25) or EU regulations[[26]](#footnote-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 have effect on the security of traffic in the port, entries and exists of ships and the implementation of the port security plan.[[27]](#footnote-27)

In 2016, a Port Cyber Resilience Officer was appointed and a plan of action was decided on. His area of responsibility includes, among other things, raising awareness, training and management of cyber risks. To this end, committees were established that deal with the various aspects of cyber security, such as law, Exercises, etc. The officer works in cooperation with law enforcement agencies, municipal authorities and other bodies.[[28]](#footnote-28) The port carries out cyber exercises and maintains a staff of cyber security experts who are responsible for protecting the port infrastructure.

Cyber security conferences have been held in order to raise awareness and improve cyber training for businesses that operate in the port. The port operates a program of cyber security assistance to small businesses, which includes online training and tools that help to identify cyber weaknesses. The assistance is provided based on the perception 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 can constitute a weak link.[[29]](#footnote-29)

The **port of Amsterdam** initiated a program to upgrade cyber security in 2018. It presented e-learning modules about information security which are intended to raise awareness of the issue among workers and other relevant entities. The port has recruited an information security officer and has established a cyber security hotline. [[30]](#footnote-30) The hotline receives reports that are not compulsory as well as those that are when the involved entities are subject to the ISPS code and fulfill a list of conditions published by the port.

Cooperation is maintained in this area with entities, such as the NCSC, the port of Rotterdam, the Digital Trust Center (DTC) and others. In addition, a program has been initiated in the port for the sharing of information with the private and public sectors, including law enforcement agencies and others. The port holds public information events in cyber security in order to raise awareness and to provide professional information.[[31]](#footnote-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, whose goal is to proposes possible solutions to cyber threats in the maritime sector.[[32]](#footnote-32)

The Canadian Cyber Incident Response Center (CCIRC) operates a digital platform for the distribution of information to critical infrastructure sectors and to enhance cooperation. The platform facilitates the distribution of information according to levels of security classification. The Center is available to assist in the management of cyber events in critical infrastructures, including in the maritime sector, and it operates support programs to help entities in the private sector carry out risk assessments.[[33]](#footnote-33)

The 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]](#footnote-34)

The federal institution Transport Canada is responsible for establishing a network for cooperation that carrying out an up-to-date sectoral risk assessment on an annual basis.[[35]](#footnote-35) Also, In 2016, Transport Canada published a document on cyber security best practices for the maritime sector.[[36]](#footnote-36) It should be mentioned that similar documents were published in 2016-2017 for the maritime sector in United Kingdom. The documents present recommended methods for cyber security in port infrastructures and shipping.[[37]](#footnote-37) France also published a series of documents in 2016-2018 on maritime cyber security[[38]](#footnote-38) and the European Union Agency for Cybersecurity (ENISA) published, in 2019, Good practices for cybersecurity in ports.[[39]](#footnote-39)

Canada has created Marine Security Operations Centers (MSOC) that are responsible for management of events in the maritime domain. In recent years, the area of cyber security has been added to the responsibility of the centers’ operations. The centers assist in the assessment of risk to ports, vessels and maritime facilities. Each year, about 7000 risks assessments are carried out for vessels entering Canada’s maritime domain.[[40]](#footnote-40)

The centers bring together various governmental bodies that are involved in the maritime domain. The centers focus on identifying and reporting maritime activity that represents a potential threat to security and safety.[[41]](#footnote-41)

**Denmark – Implementation of a maritime cyber security strategy**

The maritime sector is one of the critical infrastructures in Denmark according to its national cyber strategy. A cyber strategy document that specifically deals with the maritime sector was published in January 2019 and some of the measures appearing in it have already been implemented.[[42]](#footnote-42) The largest container shipping company in the world—A.P. Moller-Maersk—is headquartered in Denmark. A major cyber attack on Maersk in 2017 caused it damage and had an effect on the port operations in a number of countries.[[43]](#footnote-43)

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

In June 2018, a maritime cybersecurity unit was established in the DMA and it is responsible for the implementation of measures that appear in the strategy document. The Unit is meant to serve as an advisory body, a communication center for the maritime sector and a source of expertise in the DMA. The Unit is responsible for coordination of an action plan together with the maritime sector in areas such as regulation, training, raising awareness, etc.[[46]](#footnote-46) The Unit participates in a cyber forum that includes all of the cyber units in Denmark’s critical sectors and which is operated in partnership with the CFCS. The goal of the forum is to share information on threats, cyber events and to promote cooperation between the various sectors.[[47]](#footnote-47)

An order on maritime cyber security was published by the DMA and went into effect in February 2019. The order implements part of the European Union NIS directive on cyber security (Directive (EU) 2016/1148).[[48]](#footnote-48) The order includes a number of obligations that apply to bodies appointed as operator of a maritime service by the DMA. For example, in certain cases, there is an obligation to report a cyber event to the DMA and to the CFCS. Another obligation is to be certified to recognized international cyber security standard, within a period of two years from that appointment.[[49]](#footnote-49)

The DMA works to create cooperation in the cyber security field with other countries.[[50]](#footnote-50) A cyber security forum including all of the authorities that have any direct influence on the maritime sector in Denmark will come into being in 2020-2021. The forum will work to prepare plans for responding to cyber events and emergencies, to coordinate cyber exercise in the sector, etc.[[51]](#footnote-51)

**The United States – The maritime sector and the port of Los Angeles**

The US Coast Guard, the body that is responsible for cyber security in the maritime sector, published its strategy for cyber security in 2015.[[52]](#footnote-52) There is extensive regulation of maritime security in the US.[[53]](#footnote-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]](#footnote-54) The National Cybersecurity and Communications Integration Center (NCCIC) that is part of the Homeland Security Department provides assistance to critical infrastructures, including the transportation sector which the maritime sector is part of.[[55]](#footnote-55) The Center includes a Hunt and Incident Response Team (HIRT) which assists organizations that have been attacked and which request its intervention.[[56]](#footnote-56) In addition, a platform for the sharing of information has been created for the maritime sector (MPS-ISAO), which is a non-profit organizations operating as a partnership between the private and the public sectors.[[57]](#footnote-57)

The port of Los Angeles, which is ranked first in container traffic in the US, operates the Cyber Security Operations Center (CSOC) which is responsible for port infrastructure and is considered the first of its kind in the country. The port reported in 2019 that it is the only one in the country that is certified as meeting the cyber standard ISO 27001.[[58]](#footnote-58) A plan to establish a Cyber Resilience Center that will serve all of the entities connected to the port was initiated in 2019. The center is expected to serve as a platform for the sharing of information and professional knowledge, the coordination of operations, etc.[[59]](#footnote-59)

**Conclusion and Recommendations**

There are several key components in national cyber security arrays in the civilian maritime sector, as presented in this article. A summary of the components will be presented below, however, this is not an exhaustive list of all the possibilities. There are variations that can be tailored to the specific conditions and characteristics of the country. Wise use of the various tools and the establishment of an optimal cyber security structure in the maritime sector can support the effective management of the cyber domain.

As mentioned, there are a number of leading international guides which provide professional insights that can assist in the creation of a sectoral cyber security arrays. The arrays presented in this article make use of similar tools to those presented in the guides, for the most part. Guides have been published by, among others, the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCDCOE), the European Union Agency for Cybersecurity (ENISA) and the International Telecommunications Union (ITU).[[60]](#footnote-60)

Following is a list of recommended components of a national cyber security arrays in the civilian maritime sector, which are used in existing arrays worldwide and which are 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 base to assist 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.

1. A maritime cyber security body

Usually operates within a government entity that is responsible for the civilian maritime sector. This body interacts with the various entities in the maritime sector. Its function can include, among others, implementation of programs for training and raising awareness, management of Exercises in the sector, assistance and consulting, assessment of sectoral risks and threats, publishing of directives, etc.

Also a Cyber Security Operations Center (CSOC) that operates in the maritime sector will facilitate the ongoing management and rapid response to any cyber activity in the sector. The center will provide a full picture of what is happening in the sector, will coordinate the information received from the various sources, will manage the response to major cyber events, etc.

1. 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, 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 infrastructures and anyone active in the maritime sector and not included in the aforementioned categories. The programs are usually tailored to each group.

**Risk assessments**

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 which will include representatives of the body responsible for the maritime sector.

1. Forum of government entities and/or essential entities

Forum for coordination and cooperation that brings together all government bodies and critical infrastructures 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.

1. Forum for all stakeholders in the civilian maritime sector

A forum for coordination and the sharing of information and abilities that brings 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 base for the establishing of cyber bodies in the array. In addition, it will specify obligations such as the duty to report defined cyber events to the relevant government bodies. It is also recommended to establish cyber entity with powers for gathering information, issuing directives and/or standards, supervision and oversight, investigation and management pf cyber events in certain cases, etc.

**Continuity and recovery plans**

Preparation and implementing of continuity and recovery plans for the maritime sector in general and specifically for bodies and infrastructures in the maritime sector.

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). [↑](#footnote-ref-1)
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 [↑](#footnote-ref-2)
3. Cyber events have occurred in ships, offshore drilling rigs, commercial port infrastructure, energy terminals (oil and gas), shipping companies, freight forwarder 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. [↑](#footnote-ref-3)
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. [↑](#footnote-ref-4)
5. Singapore Ministry of Trade and Industry, Enterprise Singapore, Industry Profile, 2018: https://www.enterprisesg.gov.sg/industries/type/sea-transport/industry-profile [↑](#footnote-ref-5)
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/ [↑](#footnote-ref-6)
7. Lloyds list, One Hundred Ports 2019: <https://lloydslist.maritimeintelligence.informa.com/one-hundred-container->

   ports-2019 [↑](#footnote-ref-7)
8. Singapore's Cybersecurity Strategy, Cyber Security Agency of Singapore, 10 Oct 2016: https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf

   [↑](#footnote-ref-8)
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 [↑](#footnote-ref-9)
10. Singapore Computer Emergency Response Team (SingCERT), Maritime, 08 Oct 2019: https://www.csa.gov.sg/singcert/publications/maritime [↑](#footnote-ref-10)
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 [↑](#footnote-ref-11)
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 [↑](#footnote-ref-12)
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 [↑](#footnote-ref-13)
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. [↑](#footnote-ref-14)
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 [↑](#footnote-ref-15)
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 [↑](#footnote-ref-16)
17. Maritime and Port Authority of Singapore, New 24/7 Maritime Cybersecurity Operations Centre to Boost Cyber Defence Readiness, 16.5.2019. [↑](#footnote-ref-17)
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 [↑](#footnote-ref-18)
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 [↑](#footnote-ref-19)
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 [↑](#footnote-ref-20)
21. World shipping Council, Top 50 World Container Ports: http://www.worldshipping.org/about-the-industry/global-trade/top-50-world-container-ports [↑](#footnote-ref-21)
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. [↑](#footnote-ref-22)
23. Port of Rotterdam Authority, Facts and Figures, 2019: https://www.portofrotterdam.com/sites/default/files/facts-and-figures-port-of-rotterdam.pdf [↑](#footnote-ref-23)
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 [↑](#footnote-ref-24)
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 [↑](#footnote-ref-25)
26. Regulation (EC) no. 725/2004; Netherland Port Security Act: https://wetten.overheid.nl/BWBR0016991/2010-10-01 [↑](#footnote-ref-26)
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 [↑](#footnote-ref-27)
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 [↑](#footnote-ref-28)
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 [↑](#footnote-ref-29)
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 [↑](#footnote-ref-30)
31. Port of Amsterdam, Cyber security in the North Sea Canal Area (NSCA): https://www.portofamsterdam.com/en/port-amsterdam/organisation/cyber-security-nsca [↑](#footnote-ref-31)
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/ [↑](#footnote-ref-32)
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 [↑](#footnote-ref-33)
34. Transport Canada, Marine Security Operations Bulletin, No: 2014- 001: https://www.tc.gc.ca/media/documents/marinesecurity/MSOB\_BSOM\_2014-001-en.pdf [↑](#footnote-ref-34)
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 [↑](#footnote-ref-35)
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 [↑](#footnote-ref-36)
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 [↑](#footnote-ref-37)
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 [↑](#footnote-ref-38)
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 [↑](#footnote-ref-39)
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 [↑](#footnote-ref-40)
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 [↑](#footnote-ref-41)
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 [↑](#footnote-ref-42)
43. MAERSK Site, News Release, A.P. Møller - Mærsk A/S Cyber attack update, June 28, 2017: http://investor.maersk.com/node/19831/pdf [↑](#footnote-ref-43)
44. DMA, Cyber and Information Security Strategy for the Maritime Sector, page 8-9. [↑](#footnote-ref-44)
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 [↑](#footnote-ref-45)
46. Danish Maritime Authority, Danish Maritime Cybersecurity Unit: https://www.dma.dk/SikkerhedTilSoes/Cybersikkerhed/Sider/default.aspx [↑](#footnote-ref-46)
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 [↑](#footnote-ref-47)
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 [↑](#footnote-ref-48)
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 [↑](#footnote-ref-49)
50. DMA, Cyber and Information Security Strategy for the Maritime Sector, page 6-7 [↑](#footnote-ref-50)
51. Ibid, page 9-10. [↑](#footnote-ref-51)
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. [↑](#footnote-ref-52)
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

    https://www.govinfo.gov/app/details/CFR-2009-title33-vol1/CFR-2009-title33-vol1-part104 [↑](#footnote-ref-53)
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. [↑](#footnote-ref-54)
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 [↑](#footnote-ref-55)
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 [↑](#footnote-ref-56)
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 [↑](#footnote-ref-57)
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 [↑](#footnote-ref-58)
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 [↑](#footnote-ref-59)
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. [↑](#footnote-ref-60)