Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Yavor Todorov, *Connections QJ* 20, no. 3 (2021): 71-91
https://doi.org/10.11610/Connections.20.3.04

Research Article

Maritime Cyber(in)security: A Growing Threat Imperils EU Countries

Yavor Todorov

Ph.D. program, Bulgarian Naval Academy, http://www.naval-acad.bg/

Abstract: The massive incorporation of advanced information and communication technologies in ships, ports, traffic, and cargo management increases efficiencies but also creates vulnerabilities. Various malicious actors are willing to exploit access through the cyber domain to gain certain benefits. This article examines cyber risks and threats in the maritime cyber domain and reviews applicable European, US, and international norms, standards, and frameworks aiming to promote cybersecurity. The author outlines six lines of effort focusing on information sharing, awareness raising, certification, and resilience.

Keywords: maritime security, cybersecurity challenges, norms, harmonization, frameworks, information sharing, awareness, training, resilience.

The world is changed. I feel it in the water. I feel it in the earth. I smell it in the air. Much that once was is lost.[1]

Background

The maritime domain has grown significantly in the past ten years. It is currently a vast interconnected network of cargo ships, crude oil tanks, chemical tankers, container ships, passenger ships, insurance companies, offshore and shore operators, national and international authorities, military forces, navigation experts, maritime management, satellite, and communication systems. Today, the

[1] J.R.R. Tolkein, *The Lord of the Rings: The Fellowship of the Ring* (London, UK: HarperCollins Publishers, 2003).

maritime domain directly affects economic, political, and demographic dynamics on a global scale.

Catastrophic events are not foreign to the maritime industry. The Titanic, for example, sank in 1912, killing 1 517 people. However, as the maritime domain increasingly incorporates information and communication technologies (ICTs), the chance of catastrophe increases exponentially. These ICTs support essential shipping services such as navigation, engine monitoring, access control, entertainment, communication, and crew management. However, digitalization increases risks such as port or ship shutdowns, manipulation of essential services, and mass destruction, disorder, or loss of human life. These risks affect everyone, including private companies, governments, and individuals. As noted by Kathy Metcalf, president and chief executive officer of the Chamber of Shipping of the United States of America, the maritime industry remains vulnerable to cyberattacks, which could provoke catastrophic events, such as the takeover of a ship and ramming it into the Verrazano-Narrows Bridge.[2] This danger is confirmed by the increase of cyberattacks targeting the maritime domain by 400 percent in 2020.[3]

The maritime cybersecurity domain is regulated by many international and national public and private entities, such as the International Maritime Organization (IMO), the European Union Agency for Cybersecurity (ENISA), and the Baltic and International Maritime Council (BIMCO). Unfortunately, these organizations do not possess sufficient technical and human capabilities to implement, certify, and monitor the shipping cybersecurity system. Nor do they have adequate policies and procedures to enforce specific requirements.

The current regulatory framework cannot minimize the risks and threats primarily because there is no harmonization between the existing cybersecurity standards and procedures that monitor the maritime sector. IMO's International Safety Management Code, IMO's Guidelines on Maritime Cyber Risk Management, the EU's relevant guidelines, and the corresponding national norms are too broad, and the operators cannot achieve a resilient shipping cybersecurity system.

Another challenge is the lack of standardization of cybersecurity protocols across ships of different nations. This is due to the number of vessels operating in different environments and under various national flags. These vessels tend to follow minimal existing standards and ignore national maritime authorities' requirements.[4]

---

[2] John Grady, "Experts: Maritime Industry Remains Vulnerable to Cyber Attacks," *USNI News*, September 28, 2020, https://news.usni.org/2020/09/28/experts-maritime-industry-remains-vulnerable-to-cyber-attacks.

[3] "Greater Cyber Security Needed for Coronavirus and Economic Crises," *Hellenic Shipping News*, May 6, 2020, https://www.hellenicshippingnews.com/greater-cyber-security-needed-for-coronavirus-and-economic-crises/.

[4] Jeff Spivey, "Security by Design," *United States Cybersecurity Magazine* (Fall 2017), https://www.uscybersecurity.net/csmag/security-by-design/.

Many ships' informational infrastructure is set up following the "cybersecurity by design" approach. Based on this model, cybersecurity is included in the ship from its initial design and is addressed at every stage of the building process. However, this "by design" approach focuses on early warning and prevention instead of remediation and restoration after a security incident.[5] As the current attack vectors are multidimensional and use state-of-the-art tools to infiltrate systems, this model creates significant risks and challenges for the shipping industry.[6]

Numerous different equipment and service providers allow each vendor to implement unique security protections, making harmonization a significant challenge. Additionally, publicly accessible systems required to identify and locate a vessel in distress also use this technology.[7]

The potential for cyberattacks to disrupt the shipping industry is high and could provoke catastrophic damage to vessels and critical infrastructure. It is crucial that ship owners, crews, and responsible organizations enhance cybersecurity awareness in the maritime industry. Following are well-grounded recommendations for enhancing international maritime cyber security regulations, policies, and frameworks to address the current cybersecurity challenges.

The Current State of the Maritime Domain

Global seaports are increasingly important to the world economy and the European Union (EU) economy. They are the main intersections of the world trade network, as they account for about three-quarters of EU freight trade with third countries and over one-third of intra-EU freight transport.[8]

Since 1970, the world maritime trade has increased steadily, both in volume and ship size. The United Nations Conference on Trade and Development (UNCTAD) expects maritime trade volumes to expand to an annual rate of 2.4 percent by 2030. Around two-thirds of global trade in goods occurs in developing countries, accounting for sixty percent of global goods transport. Much of this growth has been in East Asia, especially China. There has also been a surge in volumes on the Transpacific trade route linking East Asia to North America.[9]

---

5 Reciprocity, "What is Security by Design?" *Reciprocity*, March 7, 2020, https://reciprocity.com/resources/what-is-security-by-design/.

6 Rory Hopcraft and Keith M. Martin, "Effective Maritime Cybersecurity Regulation – the Case for a Cyber Code," *Journal of the Indian Ocean Region* 14, no. 3 (2018): 354-366, http://doi.org/10.1080/19480881.2018.1519056.

7 Hopcraft and Martin, "Effective Maritime Cybersecurity Regulation."

8 Boyan Mednikarov, Yuliyan Tsonev, and Andon Lazarov, "Analysis of Cybersecurity Issues in the Maritime Industry," *Information & Security: An International Journal* 47, no. 1 (2020): 27-43, https://doi.org/10.11610/isij.4702.

9 United Nations Conference on Trade and Development (UNCTAD), *Review of Maritime Transport 2021* (United Nations, 2021), https://unctad.org/webflyer/review-maritime-transport-2021.

Maritime Cybersecurity Domain Analysis

Maritime industry progress relies heavily on technological innovation in digitalization aboard ships. Information systems grow more critical by the day as they facilitate communication and decision-making, enhance visibility, efficiency, and reliability, and increase security in shipping operations under various conditions.

Year	Tanker Trader	Main bulk	Other dry cargo	Total (all cargoes)
1970	1 440	448	717	2 605
1980	1 871	608	1 225	3 704
1990	1 755	988	1 265	4 008
2000	2 163	1 186	2 635	5 984
2005	2 422	1 579	3 108	7 109
2006	2 698	1 676	3 328	7 702
2007	2 747	1 811	3 478	8 036
2008	2 742	1 911	3 578	8 231
2009	2 641	1 998	3 218	7 857
2010	2 752	2 232	3 423	8 408
2011	2 785	2 364	3 626	8 775
2012	2 840	2 564	3 791	9 195
2013	2 828	2 734	3 951	9 513
2014	2 825	2 964	4 054	9 842
2015	2 932	2 930	4 161	10 023
2016	3 058	3 009	4 228	10 295
2017	3 146	3 151	4 419	10 716
2018	3 201	3 215	4 603	11 019
2019	3 163	3 218	4 690	11 071
2020	2 918	3 181	4 549	10 648

Figure 1: International Maritime Trade 1970-2020.[10]

A major event in 2017 changed how governments and private industry approach shipping and port cybersecurity systems. In June, hackers working for the Russian military security service distributed the *NotPetya* ransomware to critical infrastructure entities. By exploiting vulnerabilities in Maersk, the world's largest shipping conglomerate, the hackers impaired the Global Maritime Transport System.[11]

[10] UNCTAD, *Review of Maritime Transport*.

[11] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Following this attack, IMO published the Guidelines on Maritime Cyber Risk Management.[12] These guidelines recommend best practices regarding essential shipping services such as bridge systems, cargo handling, management systems, propulsion and machinery management, power control systems, access control systems, passenger servicing, and communication systems.[13] These services run on the following platforms:

- ECDIS (Electronic Chart Display and Information System)
- AIS (Automatic Identification System)
- Radar/ARPA (Radio Direction and Ranging/ Automatic Radar Plotting Aid)
- Compass (Gyro)
- Steering (Computerized Automatic Steering System)
- VDR (Voyage Data Recorder)
- GMDSS (Global Maritime Distress and Safety System)
- ESD (Emergency Shut Down Systems).

Technical analysis showed the following vulnerabilities in some of these systems.[14]

Table 2. Shipping Platforms Threat Analyses.[15]

Platform	Use	Vulnerability	Impact
ECDIS	Visualization of navigation charts	Lack of mechanism for authentication	Altering the route
AIS, GMDSS	Identification and distress alert	Not equipped with security and data verification mechanisms	Generating false AIS command commands and altering the ship's route
Emergency Shut Down Systems (ESD)	Block the propulsion and machinery management in case of emergency	Accessible from the shore	The vessel's machine could be stopped remotely

Source: Mednikarov et al., 2020.

[12] International Maritime Organization (IMO), "Maritime Cyber Risk," www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

[13] IMO, "Maritime Cyber Risk."

[14] Mednikarov, Tsonev, and Lazarov, "Analysis of Cybersecurity Issues in the Maritime Industry."

[15] Mednikarov, Tsonev, and Lazarov, "Analysis of Cybersecurity Issues in the Maritime Industry."

In addition, many of the new software products are not compatible with the hardware used. The most common operating system on merchant ships is Windows XP, although support from Microsoft expired in 2014. In 2015, a study in the United States found that thirty-seven percent of servers were not up-to-date and were considered potentially vulnerable to cyberattacks.[16] In 2020, these numbers were similar, as the main ship's equipment had not changed.

The main types of cyberattacks against vessels exploiting existing vulnerabilities are:

- Phishing – Sending e-mails to a large number of addressees, requiring them to fill in sensitive or confidential information. Such attacks may also prompt the user to access a particular resource to allow unauthorized access to the information infrastructure.
- Ransomware – Actions where malicious code encrypts stored data in a system and requires a ransom to decrypt it. Vessels are vulnerable to this because they lack plans for checking the files used, and most of them lack mechanisms for checking incoming and outgoing electronic correspondence.[17]
- Scanning – The process of finding vulnerabilities in a particular system.
- Denial of service – The process by which the traffic of a certain number of remotely controlled computers overloads the communication capacity or interrupts access to a particular resource or service.
- Supply chain attack – The process of malicious influence on a ship's systems through a device in which malicious code is pre-injected.
- GPS Spoofing – The process when an attacker tricks the ship's GPS receiver into changing the location display to another.
- Man-in-the-middle attack – The process when the attackers can intercept and affect the traffic between the ship and shore.

The Baltic and International Maritime Council (BIMCO)'s Guidelines on Cybersecurity Onboard Ships[18] outlines several cyber threat "actors" for ships. One type of actor is the activist. Their goal can be, among others, the destruction or publication of sensitive data to gain attention from the media or DoS (Denial of Service) and Intellectual property theft.[19] This could include an insider threat that disrupts operational services and causes reputational loss. The second type

[16] Ms. Smith, "Maritime Cybersecurity Firm: 37% of Microsoft Servers on Ships Vulnerable to Hacking," *CSO*, May 4, 2015, https://www.csoonline.com/article/2917856/maritime-cybersecurity-firm-37-of-microsoft-servers-not-patched-vulnerable-to-hacking.html.

[17] Mohamed Amine Ben Farah et al., "Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends," *Information* 13, no. 1 (2022), 22, https://doi.org/10.3390/info13010022.

[18] Baltic and International Maritime Council, 2020.

[19] IMO, "Maritime Cyber Risk."

of actors are criminals seeking financial gain through both commercial and industrial espionage. The end goal is selling and ransoming stolen data, blocking system operability, and organizing fraudulent cargo transportation. The third group, and probably the most feared, are nation-state-supported groups seeking political or military influence by negatively interfering with the targeted vessel or shipping company's essential services. A successful cyber-attack could be used to decrease the government's authority or modify the state's political goals and focus.[20] Nation-state actors tend to focus on the exfiltration of sensitive and classified data or influencing an essential service. They have almost unlimited resources and can achieve their goals without being limited by time horizons or potential financial profits. Examples of essential nation-state attacks include the cyberattacks on the election system in Estonia in 2007,[21] the cyberattacks during the Russo-Georgian War,[22] and the DDoS attacks on US banks in 2013.[23]

The most significant examples of these types of cyberattacks are shown in the table below.

Table 2. Major Maritime Cyberattacks Examples.

Type of Attack	Year	Description
Ransomware attack/ phishing attack	2021	South Korea's national flagship carrier HMM: Cyberattack, resulted in limited email system access.[24]
Ransomware attack	2020	Port near the strait of Hormuz: The attempted cyberattack damaged some operating systems at the port.[25]
Malware attack	2020	Mediterranean Shipping Company (MSC): For security issues, MSC servers were closed

[20] IMO, "Maritime Cyber Risk."

[21] Patrick Howell O'Neill, "The Cyberattack That Changed the World," *Daily Dot*, May 20, 2016, https://www.dailydot.com/debug/web-war-cyberattack-russia-estonia/.

[22] "The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict," *AFCEA*, May 24, 2012, https://www.afcea.org/committees/cyber/documents/therussogeorgianwar2008.pdf.

[23] Nicole Perlroth and Quentin Hardy, "Banking Hacking was the Work of Iranians, Officials Say," *The New York Times*, January 8, 2013, https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

[24] Naida Hakirevic Prevljak, "HMM Hit by Cyber Attack," *Offshore Energy*, June 15, 2021, https://www.offshore-energy.biz/hmm-hit-by-cyber-attack/.

[25] Tzvi Joffre, "Cyber Attack Targets Iranian Port near Strait of Hormuz," *The Jerusalem Post*, May 11, 2020, https://www.jpost.com/breaking-news/cyber-attack-targets-iranian-port-near-strait-of-hormuz-627616.

		to protect the company's data, and, as a result, the company's website was taken down.[26]
Malware attack	2019	The attack targeted a US vessel, causing critical credential mining. The Coast Guard and the FBI reported that the lack of security on the ship was the main reason for such an attack: all crew on the vessel shared the same login and password for the vessel's computer. Moreover, the use of external devices facilitated the task of the hacker. Another critical mistake is the lack of antivirus software.[27]
Phishing attack	2019	Hackers obtained unauthorized access to James Fisher and Sons Plc (UK).[28]
Ransomware attack	2018	Chinese hackers had attacked US Navy contractors.[29]
Petya Ransomware	2017	The encrypted malware targeted all services of the Maersk shipping company. The attack named *NotPetya* affected computer servers in Europe and India. The attack severely destroyed the computers' operating system by infecting its master boot record (MBR). As a result, 17 shipping container terminals were affected, and more than 200 million USD were lost.[30]
GPS spoofing attack	2017	The attack is reported by US maritime administration. The GPS of a ship in the Russian port of Novorossiysk indicated a wrong localization.[31]

[26] Marcus Hand, "MSC Confirms Malware Attack Caused Website Outage," *Seatrade Maritime News*, April 17, 2020, https://www.seatrade-maritime.com/containers/msc-confirms-malware-attack-caused-website-outage.

[27] Davey Winder, "U.S. Coast Guard Issues Alert after Ship Heading into Port of New York Hit by Cyberattack," *Forbes*, July 9, 2019, https://www.forbes.com/sites/daveywinder/2019/07/09/u-s-coast-guard-issues-alert-after-ship-heading-into-port-of-new-york-hit-by-cyberattack/.

[28] "Marine Firm James Fisher Reports Cyber Breach," *Reuters*, November 5, 2019, https://www.reuters.com/article/us-james-fisher-cybercrime-idUSKBN1XF1SQ.

[29] "China Hackers Steal Data from US Navy Contractor," *BBC*, 9 June 2018, https://www.bbc.com/news/world-us-canada-44421785.

[30] Greenberg, "The Untold Story of NotPetya."

[31] David Hambling, "Ships Fooled in GPS Spoofing Attack Suggest Russian Cyberweapon," *NewScientist*, August 10, 2017, https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/.

Navigation systems attack	2017	A collision between the USS Fitzgerald and a container ship caused the death of seven sailors. (of the coast of Japan)[32]
GPS spoofing	2013	A research team at the University of Texas succeeded in spoofing a yacht's GPS receiver.[33]

Maritime Cybersecurity Legal Framework

To assess the factors that led to the current state of the maritime security system, we must first analyze the maritime cybersecurity framework. This section will demonstrate the unique challenges of maritime cybersecurity related to the lack of a coherent and efficient regulatory framework to minimize the risks and threats and enhance cyber resilience. It presents an overview of the international framework and the EU and US norms and regulations.

Overview of the International Maritime Cybersecurity Framework

Maritime security measures have usually been reactive to major global shocks or disasters, such as the adoption of the International Ship and Port Facility Security (ISPS) Code.[34] In response to threats to ships and ports, the ISPS Code entered into force in 2004 under Chapter XI-2 of the International Convention for the Safety of Life at Sea (SOLAS Convention), acknowledging the importance of ports in the global security domain and outlining a set of mandatory tools and recommendations to ships and port facilities.[35] This Code assumes that ensuring the safety of ships and ports is a risk management activity. Although this Code has some links to cybersecurity, such as the measures concerning access control and authentication requirements, it is primarily designed to address the physical security of the port facilities.

Another critical international norm, which has also been developed within IMO, is the Convention on Facilitation of International Maritime Traffic (FAL).[36] This convention, in force since 1967, is focused on increasing the efficiency of maritime transport. It standardizes forms to be used in the interchange of infor-

[32] Sam LaGrone, "7 Sailors Missing, CO Injured after Destroyer USS Fitzgerald Collided with Philippine Merchant Ship," *USNI News*, June 16, 2017, https://news.usni.org/2017/06/16/destroyer-uss-fitzgerald-collides-japanese-merchant-ship.

[33] Brian Dodson, "University of Texas Team Takes Control of a Yacht by Spoofing Its GPS," *New Atlas*, August 11, 2013, https://newatlas.com/gps-spoofing-yacht-control/28644.

[34] International Maritime Organization (IMO), "SOLAS XI-2 and the ISPS Code," https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx.

[35] IMO, "SOLAS XI-2 and the ISPS Code."

[36] International Maritime Organization (IMO), "FAL Convention," 1967, www.imo.org/en/OurWork/Facilitation/Pages/FALConvention-Default.aspx.

mation in the maritime-port sector, particularly concerning communication between ports and ships.[37] In order to provide FAL with adequate applicability, it was updated in 2019. It included requirements that public authorities introduce systems that enable the electronic exchange of information between ships and ports.[38] A significant innovation of this convention is that it encourages the use of a "single window" concept, in which all the stakeholders exchange data via a single point of contact. The drawback is that if an attacker gains access to any of the entry points, he gains access to the whole network.

In 2017, IMO adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems (SMS).[39] The resolution states that an approved SMS should consider cyber risk management following the objectives and functional requirements of the International Safety Management Code (ISM Code).[40] It further encourages national authorities to ensure that cyber risks are appropriately addressed in Safety Management Systems in the company's Document of Compliance as of January 1, 2021. If it is not addressed, the vessel is treated as not sea safe, and therefore, it is considered a global maritime threat.

A paramount IMO document explicitly addressing maritime cybersecurity is the IMO document entitled Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/ Circ.3), approved at the 41st session of the FAL Committee.[41] Essentially, this document recognizes that the maritime domain needs to raise cybersecurity awareness and implement specific recommendations to enhance its cyber resilience.[42] The guidelines do acknowledge that each stakeholder in the maritime industry is different. Therefore, each should implement the most relevant requirements stipulated by the flag state administration for their needs. The Guidelines[43] also encourage implementing international security standards such as ISO/IEC 27001,[44] which specify requirements for an information security management system. The Guidelines take note of industry best practices and incorporate five elements: identification, protection, detection, response, and recovery. A new element in this regulation is connected to the possibility of the vessel

37 IMO, "FAL Convention," 1967.

38 International Maritime Organization (IMO), "FAL Convention," 2017, www.imo.org/en/OurWork/Facilitation/Pages/FALConvention-Default.aspx.

39 IMO, "Maritime Cyber Risk Management in Safety Management Systems," Resolution MSC.428(98), adopted on June 16, 2017, https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf.

40 IMO, *ISM Code: International Safety Management Code with Guidelines for Its Implementation* (London, UK: IMO Publishing, 2018).

41 IMO, "Maritime Cyber Risk."

42 Akash Rana, "Commercial Maritime and Cyber Risk Management," *Safety & Defense* 5, no. 1 (2019):46-48, https://doi.org/10.37105/sd.42.

43 IMO, "Maritime Cyber Risk."

44 International Organization for Standardization (ISO), "ISO/IEX 27001: Information Security Management," 2013, www.iso.org/isoiec-27001-information-security.html.

being found unseaworthy if the recommendations are not implemented.[45] Although the IMO Guidelines on Maritime Cyber Risk Management offer recommendations to protect ships from current cyber risks and threats, they do not offer specific guidance on how to secure the communication channels between the port and vessel. Another major challenge is that the control over the implementation is linked to the flag state and the national maritime authority.[46]

To enhance interoperability, IMO implemented, in collaboration with the International Electro-Technical Commission (IEC), a new standard for maritime navigation and radio-communication equipment and systems: IEC 63.154 "Cybersecurity – General Requirements, Methods of Testing and Required Test Results."[47] This standard implements requirements, methods of testing, and standards for shipborne equipment to provide a basic level of protection against cyber incidents.

Overview of the European Union Maritime Cybersecurity Regulatory Framework

On the strategic level, the EU's driving efforts are built around the EU Security Union Strategy for 2020-2025.[48] This strategy asserts that cyberattacks and cybercrime continue to rise, and its primary goals are to increase the whole-of-society approach to security. This includes sector-specific initiatives to tackle the specific risks faced by critical infrastructures such as transport and maritime.

The general effort to secure the EU's maritime transport is supported by Directive (EU) 2016/1148, also known as the NIS Directive.[49] It was created to increase the security of networks, services, and information systems.[50] The NIS Directive aims to build cybersecurity capabilities across the EU, mitigate threats to network and information systems used to provide essential services in critical sectors and ensure the continuity of such services after cybersecurity incidents.[51]

---

[45] IMO, "Maritime Cyber Risk."

[46] Nineta Polemi, *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains* (Amsterdam: Elsevier, 2017).

[47] International Electrotechnical Commission (IEC), "IEC 63154:2021 – Maritime navigation and radiocommunication equipment and systems – Cybersecurity – General requirements, methods of testing and required test results," accessed May 13, 2021, https://webstore.iec.ch/publication/61003.

[48] European Commission, "About the European Security Union," https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en.

[49] "NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," Document 32016L1148, *EUR-Lex*, July 19, 2016, https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[50] "NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016."

[51] "NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016."

It is stressed in the Directive that the growing interdependencies between the different essential services could disrupt entities and sectors and have cascading negative impacts on the delivery of services across markets. Accordingly, the member states' essential service operators should do everything in their power to manage the risks of being attacked and further report to the authorities if there is a cybersecurity breach.[52]

The NIS Directive requires every EU Member state to identify operators of essential services with an establishment on their territory to achieve its goals. A critical factor in the NIS Directive's lack of efficiency is the broad criteria to identify these Operators of Essential Services (OES). The requirements are as follows:

- An entity provides a service that is essential for the maintenance of critical societal and economic activities
- The provision of that service depends on network and information systems
- An incident would have significant disruptive effects on the condition of that service.[53]

The application of these criteria depends on the risk assessment of the national authority to the specific essential service. In other words, although transport is identified as a critical service for the EU, some member states could decide that some of their maritime infrastructures do not meet the criteria. Consequently, not all the ports and vessels in the EU are classified as critical infrastructure.

Another characteristic of the EU's maritime domain is the diversity of the national maritime competent authorities. Different entities, shown in the table below, have specific goals, regulatory frameworks, partners, and budgets, which creates further incoherence in the domain.

To respond to the growing threats posed by digitalization and the surge in cyberattacks, the EU Commission has submitted a proposal to replace the NIS Directive, strengthen the security requirements, and introduce more stringent supervisory measures and stricter enforcement requirements, including integrated sanctions across the European Union.[54] By adding many new sectors to the list of essential services, NIS 2 will address the security of supply chains and harmonize the reporting obligations.

[52] ENISA, https://www.enisa.europa.eu.

[53] "NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016."

[54] European Parliament, "The NIS2 Directive: A High Common Level of Cybersecurity in the EU," EU Legislation in Progress, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf.

Table 2. EU National Competent Authorities.[55]

Country	Competent Authority
Belgium	Federal Mobility Minister (Federal Public Service Mobility)
Croatia	Ministry of the Sea, Transport, and infrastructure
Czechia	National Cyber and Information Security Agency (NCISA)
Bulgaria	Ministry of Transport
Denmark	The Danish Transport, Construction, and Housing Authority
Estonia	Information System Authority (RIA)
Finland	Finnish Transport and Communications Agency Traficom
France	National Cybersecurity Agency ANSSI
Germany	Federal Office for Information Security (BSI)
Greece	National Cyber Security Authority (General Secretariat of Digital Policy - Ministry of Digital Policy, Telecommunications, and Media)
Hungary	National Directorate General for Disaster Management
Ireland	National Cyber Security Centre (NCSC)
Latvia	Ministry of Transport
Lithuania	Ministry of National Defence
Luxembourg	Institut Luxembourgeois de Régulation
Malta	Malta Critical Infrastructure Protection Unit (CIP)
Netherlands	Ministry of Infrastructure and Water Management
Poland	Ministry of Marine Economy and Inland Navigation
Portugal	National Cyber Security Centre Portugal
Romania	CERT-RO
Slovakia	Ministry of Transport and Construction of the Slovak Republic
Slovenia	Information Security Administration
Spain	Secretary of State for Security, -Ministry of Interior-, through the National Center for the Protection of Infrastructures and Cybersecurity (CNPIC)
Sweden	Swedish Transport Agency

[55] ENISA, "National Competent Authorities for the Water transport subsector," https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/nis-visualtool.

NIS 2 has the following main objectives:

- Increase the level of cyber resilience of EU country services by putting in place rules that all public and private entities responsible for those services are required to take.
- Reduce inconsistencies in resilience across the internal market in the important service sectors by further aligning the security and incident reporting requirements and the governing national supervision and enforcement.
- Improve the level of collective situational awareness and the collective capability to prepare and respond by taking measures to increase trust between competent authorities. Share more information and set rules and procedures in the event of a large-scale incident or crisis.[56]
- Improve the way the Member States draw up lists of operators of essential services by suggesting a standard set of criteria.

The backbone of protection and cyber resilience is set up around the European NIS cooperation groups' taxonomy of large-scale cyber incidents,[57] which defines all the potential malicious acts and further links them to the relevant EU political crisis response regulations. Other norms used to mitigate the risks and threats to the European maritime industry include the European Program for Critical Infrastructure Protection (EPCIP)[58] and the Directive on the Identification and Designation of European Critical Infrastructures.[59] Recently, the Proposal for a Directive on the resilience of essential entities has provided a more focused approach to critical infrastructure protection.[60]

Specific maritime cybersecurity regulatory means are built around the EU's Maritime Security Strategy (EUMSS).[61] This strategy identifies the marine security risks and threats of "*terrorism and other intentional unlawful acts at sea and in ports against ships, cargo, crew and passengers, ports and port facilities and*

[56] ENISA, https://www.enisa.europa.eu.

[57] The NIS cooperation group consists of representatives of EU member states, ENISA and the European Commission. It was established on the basis of Article 11 of the NIS Directive.

[58] European Programme for Critical Infrastructure Protection.

[59] "Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance)," Document 32008L0114, *EUR-Lex* December 23, 2008, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114.

[60] "Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities," Document 52020PC0829, *EUR-Lex*, December 16, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN.

[61] Council of the European Union, "Maritime Security Strategy," June 26, 2018, https://ec.europa.eu/oceans-and-fisheries/ocean/blue-economy/other-sectors/maritime-security-strategy_en.

critical maritime and energy infrastructure, including cyberattacks."[62] EUMSS was adopted in 2014 and revised in 2018 as a shared and comprehensive tool to identify, prevent and respond to any challenge that affects the security of European people, activities, and assets in the maritime ecosystem. The revision of the EUMSS, as adopted by the General Affairs Council on June 26, 2018, aims at a more focused reporting process to enhance awareness and better follow-up to the strategy.

To implement the regulatory framework, the EU has set up specialized entities such as the European Union Agency for Cybersecurity (ENISA),[63] The European Cyber Crime Centre (EC3)[64] at Europol, and the Computer Emergency Response Team (CERT-EU).[65] The Directorate General for Mobility and Transport (DG MOVE) and the European Maritime Safety Agency (EMSA) perform general control over the national authorities in implementing the requirements. Moreover, the EU has launched initiatives to increase cybersecurity in various critical sectors. In particular, the Information Sharing and Analysis Centers (ISAC)[66] are intended to be trusted entities to foster information sharing and good practices about physical and cyber threats and their mitigation. However, currently, the EU lags in creating ISACs for the maritime domain.

An essential program for the EU countries was presented to the Member States in March 2021. "The Digital Compass 2030"[67] aims to implement specific procedures to enhance the EU's digital transformation, improve its digital sovereignty and policies, and address vulnerabilities and threats. The program should support digitalization and increase sharing in the maritime domain by implementing state-of-the-art cybersecurity measures. The "Digital Compass 2030" is based on four key points:

- The digital empowerment of the population
- The enhancement of digital infrastructures connectivity and performance
- The digital transformation of businesses
- The digitalization of public services.[68]

---

[62] Council of the European Union, "Maritime Security Strategy."

[63] ENISA, https://www.enisa.europa.eu.

[64] "European Cybercrime Centre – EC3: Combating Crime in a Digital Age," *Europol*, updated March 1, 2022, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

[65] "CERT-EU – The Computer Emergency Response Team for the EU institutions, bodies and agencies," https://cert.europa.eu/.

[66] "Information Sharing and Analysis Centers (ISACs)," https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

[67] "2030 Digital Compass: The European Way for the Digital Decade," *EU4Digital*, March 9, 2021, https://eufordigital.eu/library/2030-digital-compass-the-european-way-for-the-digital-decade/.

[68] "2030 Digital Compass."

Fundamentally, the "Digital Compass 2030" is a clear demonstration of the EU's ambitions to implement additional cybersecurity policies and strategies and provide other tools to improve digitalization and the EU's economic and societal metrics.

The major challenge for the Member States is implementing the EU regulations. Currently, most Member States do not possess the technical capabilities and capacities to monitor the maritime critical information infrastructure, nor have they implemented specific rules to protect their relevant essential services. Other deficiencies are the lack of effective platforms and venues to share best practices and strengthen the collaboration between the Member States and their international counterparts, such as public-private partnerships.[69]

Another major obstacle in pursuing an efficient level of cyber resilience in the EU is applying penalties to those entities that are not compliant with the requirements. However, because of the lack of national will across the Member States, the penalties are, in most cases, irrelevant and inapplicable.[70]

Overview of the US Maritime Cybersecurity Framework

US maritime cybersecurity framework does not differ fundamentally from the EU's approach. The US National Maritime Cybersecurity plan regulates maritime cybersecurity. Its principles are:

- Freedom of the seas
- Facilitation and defense of commerce to ensure the uninterrupted flow of shipping
- Facilitation of the movement of desirable goods and people across borders while screening out dangerous people and materials.[71]

The plan unifies maritime cybersecurity resources, stakeholders, and initiatives, mitigating current threats, vulnerabilities, and complements.[72]

Other US policies on cyber measures for the maritime domain are the Navigation and Vessel Inspection Circular No. 01-20 "Guidelines for addressing a cyber risk at maritime transportation security act" (MTSA)[73] and a Commercial

[69] Cecilia Gondard and Enrique Guerrero Salom, "The Problem with Public-Private Partnerships and the Role of the EU," *Eurodad*, December 4, 2018, https://www.eurodad.org/PPPs-EU.

[70] This issue is addressed in the NIS2.

[71] "National Maritime Cybersecurity Plan to the National Strategy for Maritime Security" (The White House, December 2020), https://www.hsdl.org/?view&did=848704.

[72] "National Maritime Cybersecurity Plan to the National Strategy for Maritime Security."

[73] U.S. Coast Guard, "Navigation and Vessel Inspection Circular (NVIC) No. 01-20 – Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities," February 26, 2020, https://www.dco.uscg.mil/Our-Organization/NVIC/Year/2020/.

Vessel Compliance Work Instruction – CVC-WI-018(1).[74] These policies set deadlines for vessels and waterfront facilities to incorporate cyber protection activities into their security assessments and plans.

A critical challenge for the United States Coast Guard, the national maritime authority of the United States, is creating specific policies and unilaterally assessing the cybersecurity infrastructure's strength and "hardness." This is related to the lack of sharing and reporting, as well as a lack of capacities and procedures to evaluate the level of vulnerability.

A significant challenge for the international and regional maritime cybersecurity frameworks is how to minimize the threats to the ports and the cargo deriving from vessels using "flags of convenience" (FOC). These flag registries do not have specific nationality requirements for the shipping companies that use their flag.[75] According to UNCTAD, almost seventy-three percent of ships are flagged in a country different than the vessels' owner.[76] The problem is that despite having ratified several international maritime and labor conventions, FOCs often lack the resources or the will to enforce international maritime security and cybersecurity regulations effectively. Hence, they create a critical vulnerability to the whole maritime transportation system.

To summarize, the main challenges to the efficiency of the current regulatory framework are connected to the following key factors:

- Lack of harmonization and standardization between the existing frameworks
- Lack of will to enforce implementation of effective cybersecurity tools and sanctions in the case of non-compliance
- Lack of cyber awareness.

Examples

Fortunately, despite all the difficulties and challenges, some examples show that cyber resilience and cyber awareness are possible. The Norwegian Maritime Authority has warned ship owners and shipping companies that hackers have been using social media such as LinkedIn, Facebook Messenger, and WhatsApp to install malware. They issued specific recommendations to the ships and succeeded in reducing the potential impact of cyberattacks.[77]

---

[74] USCG Office of Commercial Vessel Compliance (CG-CVC), "Commercial Vessel Compliance Work Instruction – CVC-WI-018(1)2020," September 1, 2020, www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/CG-CVC/CVC_MMS/CVC-WI-018(1).pdf.

[75] "Flags of Convenience," *NGO Shipbreaking Platform*, https://shipbreakingplatform.org/issues-of-interest/focs.

[76] "Review of Maritime Transport," *UNCTAD*, https://unctad.org/topic/transport-and-trade-logistics/review-of-maritime-transport.

[77] Norwegian Maritime Authority, https://www.sdir.no/en/.

The Shipowners Claims Bureau, Inc. created a novel way of training staff both onboard and at port terminals through a cartoon booklet entitled Cyber Awareness. Cartoon figures and humor explain how seafarers need to be conversant in cyberattack countermeasures, whether ransomware or phishing hacks.[78]

Some EU Member States have embedded cyber awareness initiatives in their National Cybersecurity Strategies (NCSS). In Croatia, these initiatives cover electronic communication, critical information infrastructure, and cybercrime.[79] In the NCSS of the Czech Republic, it is covered in a separate chapter titled "Resilient Society 4.0."[80] The Estonian NCSS implements specific means to raise awareness among citizens, prevent cybersecurity incidents, and notify citizens about possible threats.[81] The primary objective of Poland's Cybersecurity Strategy is to increase the level of resilience to cyber threats. It includes specific cybersecurity awareness programs.[82]

ENISA's cyber risk management tool for ports is another example of the beneficial effect of maritime collaboration. The tool allows port operators to conduct a cyber risk assessment with a four-phase approach following common risk management principles. Moreover, the operators identify security measures based on their priorities and assess their maturity in implementing these measures.[83]

Regarding maritime sharing, the United States uses ISACs to share cyber threat information between various stakeholders. The US maritime sector has three additional ISACs (MPS-ISAO, Maritime ISAC, and the maritime transportation system ISAC).[84]

Response

Since the digitalization and implementation of ICT into merchant shipping, vessels are challenged by cyber-related risks and threats. The merchant maritime

[78] Shipowners Claims Bureau, Inc., "Shipboard Safety Cartoon," https://www.americanclub.com/files/files/Shipboard_Safety.pdf.

[79] "The National Cybersecurity Strategy of the Republic of Croatia," Zagreb, October 7, 2015 (Official Gazette No.108/2015), https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf.

[80] "Czech Republic Cybersecurity," *International Trade Administration*, accessed May 13, 2021, https://www.trade.gov/market-intelligence/czech-republic-cybersecurity.

[81] Ministry of Economic Affairs and Communications, *Cybersecurity Strategy, Republic of Estonia 2019-2022*, https://www.mkm.ee/media/703/download.

[82] Waldemar Kitler, "The Cybersecurity Strategy of the Republic of Poland," in *Cybersecurity in Poland*, ed. Katarzyna Chałubińska-Jentkiewicz, Filip Radoniewicz, and Tadeusz Zieliński (Cham: Springer, 2022), https://doi.org/10.1007/978-3-030-78551-2_9.

[83] "Cyber Risk Management for Ports," *ENISA*, https://www.enisa.europa.eu/cyber-risk-management-for-ports#/.

[84] Jaikumar Vijayan, "What is an ISAC or ISAO? How These Cyber Threat Information Sharing Organizations Improve Security," *CSO*, July 26, 2021, www.csoonline.com/article/3406505/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html.

shipping environment is currently occupied by a variety of stakeholders and controlled by many regulatory entities, each using different norms. As a result of the lack of cyber awareness and state-of-the-art technical capabilities to monitor the vessel's information infrastructure, and because the existing norms are broad or not compulsory, maritime shipping is vulnerable to a cyberattack which could cause considerable damage.

The first and most important program should be focused on improving maritime threat sharing in the maritime domain. This could be accomplished by utilizing Information Sharing and Analysis Centers (ISACs) and promoting public-private partnerships. The second program should enhance cyber awareness in the whole maritime domain. This could be accomplished by organizing specific exercises, seminars, and conferences for the whole-of-maritime domain stakeholders. Moreover, training and certifications can be included and conducted throughout the year by government authorities that regulate and standardize the process. Both initiatives are essential elements of the EU NIS 2 Directive.[85]

The third program should be dedicated to standardizing the existing legal framework. This could be accomplished by implementing a Global Maritime Cybersecurity Code, which would be easier to monitor and enforce. Moreover, a Global Code would harmonize the existing best practice in cybersecurity standards. As these standards already have international acceptance, compliance should meet less resistance from the ship owners and the national authorities. A Maritime Cybersecurity Code should have both mandatory and voluntary components. The mandatory section should be focused on ensuring the essential services of the ships. The voluntary section should cover the ways of implementing additional security measures. A sub-program should cover the FOC's accreditation and certification by implementing additional compulsory requirements to their information infrastructure. Moreover, the Maritime Cyber Code should have specific guidelines and procedures to attribute and further sanction the perpetrators of a cyberattack.

The fourth program should set up early detection capabilities for disruptive cyber events. Early detection could take many possible forms, including monitoring networks and data flows. On the operational level, this program should also include secured capacities for sharing between parties and effective means to guarantee the business continuity of the vessel. Cyber resilience should include clear plans for alternate communication channels, alternate informational databases fully independent from daily systems, and alternate tools and systems onboard vessels to guarantee that essential vessel services run continuously if the systems are breached. This program could be accomplished via EU and US-specific programs and funds.

The fifth program should counter the lack of skills in detecting a cybersecurity attack. The training should ensure that everyone can detect abnormal system behaviors and report them in a specific order. Moreover, the crew must be

[85] European Parliament, "The NIS2 Directive."

trained to follow strict cyber hygiene rules, including sophisticated authentication methods, limited access to resources, and verification of portable memory.

Finally, the last program should be focused on the recovery and reconstruction of the capabilities after a cyber incident. This could include specific exercises and training to restore essential vessel services, data restoration, incident response, and digital forensic activities. An essential aspect of this program should be based on the compensation of "the victims," whether through liability insurance or government payments. Adequate compensation reduces societal risks and damages and contributes to the economy's recovery, social stability, and trust in institutions.

Conclusion

In conclusion, the maritime cyber domain is a Titanic heading towards an iceberg. Without proper foresight and the ability of leaders in the maritime community to address its emerging vulnerabilities, it will only be a matter of time before a maritime cyberattack catastrophically affects the global maritime transport system. Although the research has identified that different entities have recognized threats to the shipping cybersecurity system in the specific norms and policies, the examination revealed that global cyber resilience had been affected lightly. In this regard, the international maritime community, supported by the regional and national maritime authorities, should execute a comprehensive program focusing on enhancing cyber awareness and harmonizing the existing regulatory framework to counter the threat. The success of such a program depends on all maritime community actors actively decreasing their cyber vulnerabilities and countering the respective risks and threats. Only then can the iceberg be avoided.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgment

Connections: The Quarterly Journal, Vol. 20, 2021, is supported by the United States government.

About the Author

Yavor Todorov is a Marshall Center Alumni Scholar, a senior Expert at the State Agency for National Security /DANS/ of Bulgaria, and leads a unit in the Cybersecurity Department. Mr. Todorov has 20 years of experience in Bulgarian security services and has held various positions, including in the area of counterterrorism, counterintelligence, and cybersecurity, for the past eight years. Mr. Todorov is an ex-naval officer who has taken part in a number of multinational exercises aimed at strengthening security in the Black Sea region. He is a member of the Horizontal Working Party on Cyber Issues at the Council of the EU and drafted the National Cybersecurity Act and the related regulations. Currently, his team is executing vulnerability assessments on the national critical information infrastructure. In addition, he works closely with Bulgaria's partnering law enforcement agencies and services. Besides English, he speaks Italian and Russian languages. He holds an MSc degree in Telecommunications and Port Management from the Bulgarian Naval Academy and an MA in Strategic Studies from National Defense University, Washington DC. He is currently finishing his dissertation on Maritime Cybersecurity.