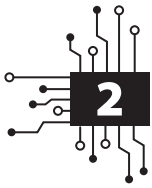

# 2 Cyber Threats to Commercial Maritime Order

BRUCE JONES

Crises can be revealing. When the *Ever Given* ran aground in the Suez Canal in March 2021, consumers worldwide saw images of bulk ships lined up for miles at the entrance to that key global chokepoint. It did more than any library of analyses to explain how globalization works. Amid the COVID-19 disruption to global markets, Americans experienced an education in U.S. reliance on global supply chains through inflation as container ships stacked up off California's coast. The threat of global famine caused by Black Sea combat illuminated global world food markets. And each of these crises highlighted the same vital point: global supply chains move by sea.

Globalization is primarily a maritime enterprise. Eighty-five percent of the world's trade moves by sea, as does two-thirds of the world's supply of oil and gas.[1] One-third of American gross domestic product and more in core allies like Britain depend on these globalized goods transport. This seaborne global economy is a gargantuan target for offensive cyber operations.

Relative to the potential massive economic damage, the system is digitally underprotected. Three dynamics of the maritime industry are shaping the issue: its increasing technological adoption from a low base, partial centralization, and rapid growth in the number and sophistication of cyber attacks.

## TECHNOLOGIC STATE OF THE GLOBAL MARITIME SYSTEM

Far more so than any national navy, the commercial shipping enterprise draws on a complex mix of ship builders, owners, and operators; freight forwarders and local transport companies; port operators, stevedores' associations, crane operators, and pilots; and global multinationals. It operates through myriad authorities at the local, state, national, transnational, and global level. And as many as a dozen insurance regimes cover different aspects of the movement of goods by sea.

For this system to function smoothly, dozens of information systems interact on an hour-by-hour (and in some cases, minute-by-minute) basis occurring over hundreds of ports worldwide, in more than 150 countries, each with their own information systems, regulations, and sovereign authorities. It is a complex, multisector, multidomain, multinational "system of systems of systems" operating at a genuinely global level. (See related discussion of the global cyber substrate by Demchak and of the maritime transportation system by deWitte and Lehto in this volume.)

That complexity means that there are hundreds of thousands of potential entry points for cyber penetration or attack because this massive maritime transportation system (MTS) is also surprisingly low-tech beyond the engine rooms or navigation software of modern container ships. But the sector is slow to adopt new technologies, especially in the handling of cargo where bills of lading may be filled by hand and shared by fax or by exchanging thumb drives. Even the most high-tech ship must be able to interact with that low-tech system. The more sophisticated large global shipping companies that dominate the system have operated essentially as intermediaries between freight forwarders, port authorities, and local transporters. Nonetheless, some of those information management systems are rudimentary, and manual uploading of software is routine.[2]

## PARTIALLY CENTRALIZED DATA MANAGEMENT

A fluid network that globally links international MTS over hundreds of thousands of individual transponders and receivers is not managed by a central authority. It operates within standards set by the International Maritime Organization (IMO), but there is no coordinated effort among international

coast guard authorities or globally enforceable formal mechanisms to enforce digital security such as encryption or verification protocols.[3] And it relies on many intermediate receivers operated by low-tech ports and local boating clubs, and occasionally staffed by volunteers.

For example, integrated into most global shipping is the global positioning system–based and ship-identifying automated information system (AIS) transponder by which almost all commercial ships send maritime very high-frequency (VHF) data to nearby ships, ground-based receivers, and satellites.[4] (Naval ships turn them on and off as needed.) The AIS system is one of the most consequential and most vulnerable points of entry for cyber attack.

AIS transmits the name, number, location, speed, and heading of the ship every several seconds while sailing and every few minutes at anchor, and periodically sends additional information such as the ship's IMO identification number, dimensions, and estimated time at destination. With at least eighty thousand ships at sea at any one time, each sending around ten pieces of data every six seconds, the AIS system shares billions of pieces of data per day.[5] A VHF antenna attached to the International Space Station supports the network.[6]

The maritime commercial sector becomes more centralized in the five mega-firms accounting for 70 percent of all global shipping. Maersk, Mediterranean Shipping Company, CMA/CGM Group, Cosco Shipping Holdings Company, and Hapag-Lloyd are highly sophisticated entities themselves. Within their own centralized conglomerates, then, they are able to drive technological advances.[7]

## ⊢• RISING CYBER THREATS TO MARITIME OPERATIONS

Estimates are that by 2023, there had been a 400 percent increase in cyber attacks by nonstate actors since 2020.[8] In July 2018 COSCO suffered an attack on its phone and email systems that disrupted business operations in North America.[9] In the same time period, a virus infected the main software system of DNV Maritime, the world's largest provider of classification, software, and certification systems to the commercial shipping fleet.[10] A malware attack hit the Mediterranean Shipping Company in April 2020, causing its main data center in Geneva to be closed for six days, at a cost to the company of several

hundred million dollars.[11] An early 2023 ransomware attack came from the notorious group LockBit, which took possession of all of the data of the port of Lisbon and threatened to release that data if a ransom was not paid.[12]

The largest cyber disruption to the commercial maritime industry so far, however, originated with a state actor—Russia. The 2017 NotPetya campaign was a Russian attack on Ukrainian tax management software (MeDoc), but the malware spread to other nations' commercial entities like the massive Danish shipping firm Maersk.[13] From there, it infected the entirety of the world's largest shipping firm, which moved one in five containers representing roughly 15 percent of global trade. Unusable for several days were fifty thousand laptops, four thousand servers, and seventeen terminals globally, with $10 billion in damages over all affected entities.[14] The company itself estimates $300 million in direct losses from the attack, not including later information technology (IT) upgrade spending and expanding from eight hundred to six thousand IT personnel.[15] A two-minute cyber attack on Maersk's systems cost more than all Somali piracy attacks combined.[16]

Maersk, both as primary victim and largest entity in the system, began efforts not just to recover from the attack but also to build a sophisticated system for the entire industry, TradeLENS.[17] Built in collaboration with IBM Blockchain, it aimed to provide a one-stop, cloud-based data center for ports, port operators, ship operators, and commercial maritime networks. If fully adopted, TradeLENS would have put two well-resourced, sophisticated entities at the heart of cyber defense for the global maritime industry. However, it would also mean far greater centralization in the industry, reversing its low-tech, distributed feature, which, under some circumstances, provides a source of resilience for highly complex systems. (See discussions of systemic cyber resilience in this volume by Ross and Warner, and Demchak.) In any event, the industry was not ready to adopt a system-wide platform, and in November 2022, Maersk and IBM quietly shelved the program.[18] Interviews with shipping executives suggest that a major obstacle was industry hesitation to share data into a pooled system—a continuing challenge common across all collective cyber defense proposals.

Beyond NotPetya, the Houthis' Red Sea navigation attacks, and the Russian-Ukrainian war, no other significant deliberate state-based cyber attacks on a

major shipping firm are known in open sources. One possible deterrent is that the average container ship carries cargo from different economies via complex global supply chains, and, for the most part, ship operators do not know what is on their ships (the exception is hazardous material).[19] Though detailed data on these attacks is classified, however, port operators and international coast guard officials note increasing Chinese, Russian, North Korean, and Iranian cyber probes of U.S. and Western ports to test cyber defenses and gather data. Others are in effect "test runs" at wider attacks on critical infrastructure.

In the United States, with its complicated system of different authorities for foreign defense and domestic law enforcement, the Coast Guard performs an important bridging function: operating as an armed service and part of the Department of Defense (DOD) cyber defense (and increasingly, offense) infrastructure with its own Coast Guard Cyber Command but also within the Department of Homeland Security system for homeland cyber protection. (See chapter in this volume by Koch.) The ability to move between foreign and domestic authorities is particularly useful in the world of commercial shipping. The lines of global shipping ownership, however, are generally transnational, and at any given time, less than 10 percent of the ships docked in U.S. harbors are American-owned. And most democratic countries' economies rely heavily on the flow of goods in and out of ports on ships they do not own or regulate. Of course, any national authority can stipulate host port privileges to insist on various safety—including cyber safety—protocols for ships entering their waters. But that is a far weaker tool than direct regulatory authority.

Indeed, the genuinely global and transnational nature of the industry poses a serious challenge for regulation and cyber defense.

## ⊢• ISSUES FOR RESEARCH AND POLICY

Initiating effective regulation and maritime cyber defense requires solving a number of technical and policy issues. Leading cyber experts and institutions lie outside of, and are largely "sea-blind" to, the unusual configuration and specific threats to the global maritime system. So many cyber threats to terrestrial infrastructure exist that a focus on maritime activities seems a lower priority. But effects at sea inevitably become critical effects ashore, generating a series of critical questions unanswered for sea or even land. One

is whether responses should be centralized or decentralized to keep up with the increasing sophistication of attacks.

While very large economic entities are potential targets for consequential attacks, these sophisticated, well-resourced actors are also on the front lines of cyber defense.[20] Taking more advantage of their central systemic role and economic weight, for example, could be key to improved maritime-oriented innovations in cyber defenses. Policy action is needed for other issues including gaps in the IMO's legal framework for stronger cyber protection standards, training, and hygiene,[21] stronger national cyber legislation,[22] encryption and verification mechanisms for AIS,[23] and reviewing liability standards in maritime insurance, especially for incidents deemed to be "war-related."[24] An add-on maritime treaty has been proposed. While there are downsides to a treaty approach, it would create a single reference point through which several of the above elements could be advanced.[25] (See chapter in this volume by Klimburg and Wells.)

The second central question is, who could drive this agenda (or elements of it)? The IMO is that rare international institution where the United States is not a powerhouse because it is a commercial shipping featherweight. Two things give the United States more power (albeit informally): a reputation for driving safety standards at sea, and the vital role of access to the U.S. market in global economics.

Together with friendly countries that have greater roles in shipping per se—for example, Denmark and Norway—the United States and a "group of friends" could work to advance this agenda. But the extensive power of China within the IMO supports its hesitation to accept the expense of cyber upgrades as well as its far laxer standards in maritime safety.

More centralized cyber responses could be explored as well. One idea that has been floated: the use of a clearing house where companies, ports, and countries can share their experiences with attacks and defense—much like the well-developed global Cyber Rapid Response System for information sharing about internet attacks.[26] This entity would likely be housed by the IMO or the U.S. Coast Guard or by some sort of hybrid entity that draws on their respective authorities and capacities. The limit on this is companies' willingness to share proprietary software and defense techniques, but at the very least,

information on attacks can be shared with such a mechanism. And there are existing examples across other sectors such as national computer emergency response teams and, in the United States, the sector information-sharing and analysis centers. It might also be necessary to create a pooled fund on which low-capacity ports and firms can draw to upgrade their capabilities, which the European Union routinely does in other sectors.

An alternative approach is to incentivize the major shipping firms to take a more central role in upgrading the sector's defenses. This could be financed via the Group of Seven large economy nations or even the expanded Group of Twenty. While Maersk/IBM's experience is a cautionary tale, it is probably the case that other firms were leery of adopting a unified software package that they may have believed gave Maersk a competitive advantage. However, if several major firms were incentivized to train and equip their respective partners, it could generate a significant, industry-wide improvement in standards, training, and responses.

This idea is also behind the formation of the Cyber Resilience Alliance by major commercial IT capital goods firms. This concept is particularly relevant today, as a subset of the shipping "majors" increasingly take on "home-to-home" roles in vertical integration business strategies. They increase their leverage on the entire system for control and possibly security by absorbing freight forwarders and land-based transports into seamless global supply networks that go from initial customer all the way to final consumer.

This alternative could potentially be complemented by an expansion into the cyber realm of two existing programs run by the U.S. Coast Guard. One is the Container Security Initiative—which puts Coast Guard personnel physically and informationally present in several major ports worldwide—to enhance defenses.[27] At a maximum, this existing initiative could be turned into a container security and cyber initiative, where the same incentives (access to the U.S. market) and penalties (denials thereof, or delays) created powerful reasons for ports and their respective partners to upgrade their cyber defenses. The second initiative is the International Port Safety Program, whereby the United States helps partners develop port safety measures.[28] A limitation on this program is that it is reciprocal—if the United States wants to inspect a partner port, it is thereby also granting the right for a reciprocal inspection.

Still, the relationships developed through program partners could be used to offer an add-on cyber support within an adjusted framework that would limit other countries' access to U.S. cyber defense.

## ⊢• CONCLUSION

The global commercial shipping system—the MTS—is both the major artery of the global economy and a soft target for cyber attack. Upgrading both defenses and response capacity will warrant sustained attention, significant personnel, time, and money. There are a number of issues that need to be resolved—many of which parallel concerns of cyber networks ashore but have their own specific aspects. However, one can argue that cyber networks ashore cannot be separated from the maritime networks on which the land supply chain depends.

A primary issue is the attractiveness and effectiveness of centralized as opposed to decentralized responses. While centralization could logically appear more efficient (but possibly less resilient), there are significant business reasons why commercial shipping firms and their supporting contractors are reluctant to embrace it. This hesitation seems to put the burden of regulation onto governments, the IMO, or the U.S. Coast Guard (leading efforts by other coast guards, as noted by Kim in this volume). But it is not clear how to add effective regulation without stifling maritime competition and technical development. An intensified dialogue between the U.S. Coast Guard, other leading coast guards, and the five global shipping majors could be a starting point for fleshing out answers.

If maritime supply provides 85 percent of global trade, it should be no surprise that protecting it from cyber threats is a mammoth task, and one in which navies must be involved. The risks here are simply too large to ignore or underfund. Sustained attention to the problem by industry, governments, scholars, the cyber community overall—as well as navies—is a critical first step.

## NOTES

1. Rose George, *Ninety Percent of Everything: Inside Shipping, the Invisible Industry That Puts Clothes on Your Back, Gas in Your Car, and Food on Your Plate* (Metropolitan Books, 2013); Mark Levinson, *The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger* (Princeton University

Press, 2008); Daniel Yergin, *The New Map: Energy, Climate, and the Clash of Nations* (Penguin Press, 2020).

2. "Chinks in the Armor: Software and Communication Vulnerabilities on Ships," *GTMaritime*, 11 January 2023, https://www.gtmaritime.com/security/; Bruce Jones, *To Rule the Waves: How Control of the World's Oceans Shapes the Fate of the Superpowers* (Scribner, 2011), 110–23.
3. Syed Khandker et al., "Cybersecurity Attacks on Software Logic and Error Handling within AIS Implementations: A Systematic Testing of Resilience," *IEEE Access*, no. 10 (2022): 29493–29505, https://doi.org/10.1109/ACCESS.2022.315894.
4. Malik Shahzad Kaleem Awan and Mohammed A. Al Ghamdi, "Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS)," *Journal of Marine Science and Engineering* 7, no. 10 (October 2019): 350, https://doi.org/10.3390/jmse7100350.
5. Marine Traffic, 21 October 2021, https://www.marinetraffic.com/en/ais/home/centerx:-115.2/centery:26.7/zoom:4. On 21 October 2021 Marine Traffic reported monitoring two hundred thousand ships. This was unusual; eighty thousand to one hundred thousand is the more typical number.
6. European Space Agency, "AIS on ISS," https://www.esa.int/Enabling_Support/Space_Engineering_Technology/AIS_on_ISS.
7. Chronis Kapalidis et al., "A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships," *Journal of Marine Science and Engineering* 10, no. 10 (October 2022): 1486, https://doi.org/10.3390/jmse10101486.
8. Jasmina Ovcina Mandra, "Naval Dome: 400% Increase in Attempted Hacks since February 2020," *Off-shore Energy*, 5 June 2020, https://www.offshore-energy.biz/naval-dome-400-increase-in-attempted-hacks-since-february-2020/. The U.S. Coast Guard cites it in its updates on cyber protection: "Northern California Area Maritime Security Committee Cyber Security Newsletter," January 2022, https://www.sfmx.org/wp-content/uploads/2022–01_AMSC-Cyber-Newsletter.pdf.
9. The ownership structure here is illustrative of the industry. Shanghai-based COSCO Holdings is the parent company of COSCO Shipping North America, which in turn owns COSCO SHIPPING Terminals Shipping (North America) Inc. That entity formed a joint venture with Stevedoring Services of America and CMA Terminal Links; the resulting entity is called Pacific Maritime Services. That joint venture supplies terminal services to the Pacific Container Terminal, which is itself owned by SSA Marine, which is a subsidiary of CARRIX, a Seattle-based maritime services company, which owns the gantry cranes in the port. The port itself is a department of the City of Los Angeles, but governed by the Los Angeles Board of Harbor Commissioners, which operates as its

landlord, overseeing more than two hundred leaseholders. See Edwin Lopez, "How COSCO Responded to a Cyberattack on its Systems," *Supply Chain Drive*, 31 July 2018, https://www.supplychaindive.com/news/COSCO-cyberattack-response-timeline/529008/; "Cosco Reports Cyberattack at its U.S. Operations," *The Maritime Executive*, 25 July 2018, https://maritime-executive.com/article/cosco-reports-cyberattack-at-its-u-s-operations.

10. Mike Schuler, "DNV Confirms Ransomware Attack Impacting 1,000 Ships," *gCaptain*, 16 January 2023, https://gcaptain.com/dnv-confirms-ransomware-attack-impacting-1000-ships/; Damien Black, "Maritime Software Company Admits to Cyberattack," *Cybernews*, 10 January 2023, https://cybernews.com/news/maritime-software-company-cyberattack/.
11. George Grispos and William R. Mahoney, "Cyber Pirates Ahoy! An Analysis of Cybersecurity Challenges in the Shipping Industry," *Journal of Information Warfare* 21, no. 3 (August 2022): 59–73, https://arxiv.org/abs/2208.03607; Shefali Kapadia, "3 Years, 3 Cyberattacks on Major Ocean Carriers. How Can Shippers Protect Themselves?" *Supply Chain Drive*, 29 April 2020, https://www.supplychaindive.com/news/ocean-carrier-cybersecurity-maersk-msc-cosco/576754/.
12. Rakin Rahman, "Cyber Attack Threatens Release of Port of Lisbon Data," *Port Technology*, 3 January 2023, https://www.porttechnology.org/news/cyberattack-threatens-release-of-port-of-lisbon-data/; Matt Burgess and Lily Hay Newman, "The Unrelenting Menace of the LockBit Ransomware Gang," *Wired*, 24 January 2023, https://www.wired.com/story/lockbit-ransomware-attacks/. In that instance, the ransom demanded was trivially small by comparison to the sector—$1.5 million. Cyber defense officials interviewed for this chapter note that this is an important compliance challenge: the costs of paying off attackers can be far lower than the IT and training upgrades necessary for more effective cyber defense. Confidential interview, U.S. Government, Washington, DC, 8 February 2023.
13. Ellen Nakashima, "Russian Military Was behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes," *Washington Post*, January 12, 2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.
14. Josephine Wolff, "How the NotPetya Attack Is Reshaping Cyber Insurance," Brookings Institution, 1 December 2021, https://www.brookings.edu/techstream/how-the-notpetya-attack-is-reshaping-cyber-insurance/.
15. Grispos and Mahoney; Nakashima.
16. Grispos and Mahoney.

17. Caroline Donnelly, "Maersk Employs Cloud-First Strategy to Disrupt Competition and Build Innovation," *Computer Weekly*, 26 June 2019, 7–9, https://www.computerweekly.com/news/252465699/Shipping-giant-Maersk-on-taking-a-cloud-first-approach-to-disrupting-the-competition; author's notes, Maersk HQ, October 2019.
18. "A. P. Moller—Maersk and IBM to Discontinue TradeLENS, a Blockchain-Enabled Global Trade Platform," Maersk, 29 November 2022, https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens.
19. Notwithstanding the rhetoric of deglobalization and de-linkage, 2022 marked an all-time high in U.S.-Chinese trade volumes. "Global Trade Outlook and Statistics," World Trade Organization, 5 April 2023, 19, https://www.wto.org/english/res_e/booksp_e/trade_outlook23_e.pdf.
20. Shashi K. Shah, "The Evolving Landscape of Maritime Cybersecurity," *Review of Business* 25, no. 3 (2004): 30–36.
21. Md Saiful Karim, "Maritime Cyber Security and the IMO Legal Instruments: Sluggish Response to an Escalating Threat?" *Marine Policy*, no. 143 (September 2022), https://doi.org/10.1016/j.marpol.2022.105138; Juan Ignacio Alcaide and Ruth Garcia Llave, "Critical Infrastructures Cybersecurity and the Maritime Sector," *Transportation Research Procedia*, no. 45 (March 2020): 547–54, https://doi.org/10.1016/j.trpro.2020.03.058.
22. Chan Yan Jau, "Cyber Attacks as an Evolving Threat to Southeast Asia's Maritime Security," in *Evolving Threats to Southeast Asia's Maritime Security*, Asia Maritime Transparency Initiative, Center for Strategic and International Studies, December 2022, https://amti.csis.org/cyber attacks-as-an-evolving-threat-to-southeast-asias-maritime-security/; Dimitris Amprazis, "Top 11 Maritime Security Compromises of All Time," *Threatspan*, 27 December 2017, https://threatspan.com/2017/12/29/top-11-maritime-security-compromises-of-all-time/.
23. Khandker et al.
24. V. A. Greiman, "Defending the Cyber Sea: Legal Challenges Ahead," *Journal of Information Warfare* 19, no. 3 (2020): 68–82, https://www.jstor.org/stable/27033633.
25. Brendan Sullivan, "A Tale of Two Treaties: A Maritime Model to Stop the Scourge of Cybercrime," *Boston University International Law Journal* 39, no. 2 (Summer 2021): 143–80, https://heinonline.org/HOL/P?h=hein.journals/builj39&i=155.
26. William Loomis et al., *Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity*, Atlantic Council, October 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/raising-the-colors-signaling-for-cooperation-on-maritime-cybersecurity/.
27. U.S. Customs and Border Protection, "CSI: Container Security Initiative," https://www.cbp.gov/border-security/ports-entry/cargo-security/csi/csi-brief.

28. U.S. Coast Guard—Pacific Area, "International Port Security Program," https://www.pacificarea.uscg.mil/Our-Organization/District-14/D14-Units/Activities-Far-East-FEACT/FEACT-Maritime-Security/.