Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

CYBER STATECRAFT
INITIATIVE

RAISING THE COLORS:

Signaling for Cooperation on Maritime Cybersecurity

By William Loomis,
Virpratap Vikram Singh,
Gary C. Kessler, and
Xavier Bellekens

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

CYBER STATECRAFT
INITIATIVE

Scowcroft Center for Strategy and Security

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

Cyber Statecraft Initiative

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

Supported by

This report was produced by the Atlantic Council's Cyber Statecraft Initiative, in the Scowcroft Center for Security and Strategy, as part of the Initiative's work focused on cyber safety in partnership with Idaho National Laboratories supported by the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

Disclaimer

INL
Idaho National Laboratory

About INL

INL is part of the U.S. Department of Energy's complex of national laboratories. The laboratory performs work in each of the strategic goal areas of DOE: energy, national security, science and environment. INL's national and homeland security capabilities include industrial cybersecurity, operational technology and control systems.

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

CYBER STATECRAFT
INITIATIVE

RAISING THE COLORS:

Signaling for Cooperation on Maritime Cybersecurity

William Loomis, Virpratap Vikram Singh,
Gary C. Kessler, and Xavier Bellekens

ISBN-13: 978-1-61977-186-4

Cover image: High angle view on Cargo crane container terminal stock photo - Istock photos.

October 2021

Table of Contents

Executive Summary

Few industries are as critical to the global economy as the maritime transportation system (MTS), which is responsible for facilitatating the safe transport of seafaring passengers and, critically, the vast majority of international trade. The efficient operation of the MTS is at risk, though, as the industry is increasingly vulnerable to cyber threats. In 2020, cyberattacks targeting the MTS increased by 400 percent over the span of a few months.[1] Perhaps no incident better illustrated the sector's cyber vulnerability than when the MTS's principal international governance body, the International Maritime Organization (IMO), suffered a "sophisticated cyberattack" that took down its web-based services on September 30, 2020.[2]

The US government began to address the shortfalls in the sector's cybersecurity by releasing the National Maritime Cybersecurity Plan (NMCP) in December 2020. Like many first steps, the plan was more like a road map than an implementation plan, despite initiating several useful lines of effort.[3] This report builds and expands on these efforts across the complex MTS to present three overarching recommendations for industry stakeholders, as well as policy makers in the United States and allied states, to improve their collective cybersecurity posture within the MTS.

No global supply chain is independent of the maritime transportation sector, and most, in fact, are existentially dependent. The MTS feeds a quarter of US gross domestic product (GDP). Prior to the COVID-19 pandemic, commercial shipping moved close to 80 percent of global trade by volume and over 70 percent of global trade by value[4]—and postpandemic analyses suggestthe sector will recover strongly, even growing by 4.1 percent.[5] Beyond this substantial economic value, ports and shipping play a considerable role in projecting US and allied power across the globe.

More than containers and bulk cargo, the MTS is responsible for ships and offshore sites, and land-based terminals that are integral to the security of global energy systems. In 2016, more than 61 percent of the world's total petroleum and other liquid energy supply moved through sea-based trade.[6] No other form of transportation can move the sheer volume of goods at the competitive price point available in the MTS.[7] With ambitious renewable-energy targets being set by states like the United States,[8] the actors in the MTS will play a key role in maintaining and expanding renewable facilities. The MTS literally fuels the global economy.

Yet, maritime cybersecurity risks remain underappreciated. The uptick in cyberattacks targeting the MTS includes varieties of attacks familiar to other industries, including ransomware, phishing, and malware such as data wipers, to name a few. In combination with traditional cyber threats targeting information technology (IT) systems, reports of attacks on operational technology (OT), on ships and in ports, increased a whopping 900 percent in a three-year period ending in 2020.[9]

Part of the challenge of MTS cybersecurity is the complex structure of the sector. A "system of systems," the MTS is composed of individual ships, ports and terminals, shipping lines, shipbuilders, intermodal transport operators, cargo and passenger handlers, vessel traffic control, maritime administrators, and more. Each system has its own organizational peculiarities and dependencies.

1 "Maritime Industry Sees 400% Increase in Attempted Cyberattacks Since February 2020," *Security* magazine, October 20, 2020, https://www.securitymagazine.com/articles/92541-maritime-industry-sees-400-increase-in-attempted-cyberattacks-since-february-2020.

2 Catalin Cimpanu, "UN Maritime Agency Says It Was Hacked," *ZDNet*, October 06, 2020, https://www.zdnet.com/article/un-maritime-agency-says-it-was-hacked/.

3 Nina A. Kollars, Sam J. Tangredi, and Chris C. Demchak, "The Cyber Maritime Environment: A Shared Critical Infrastructure and Trump's Maritime Cybersecurity Plan," *War on the Rocks*, February 04, 2021, https://warontherocks.com/2021/02/the-cyber-maritime-environment-a-shared-critical-infrastructure-and-trumps-maritime-cyber-security-plan/.

4 "Review of Maritime Transport 2018," United Nations Conference on Trade and Development (UNCTAD) website, https://unctad.org/webflyer/review-maritime-transport-2018.

5 UNCTAD, *UNCTAD Review of Maritime Transport 2020* (New York: United Nations Publications, 2020), https://unctad.org/system/files/official-document/rmt2020_en.pdf.

6 "World Oil Transit Chokepoints," US Energy Information Administration (EIA) website, July 25, 2017, https://www.eia.gov/international/analysis/special-topics/World_Oil_Transit_Chokepoints.

7 Business Wire press release, "Global Marine Fuel Market (2020 to 2025)–Featuring Shell, Neste, and BP among Others–ResearchandMarkets.com," Associated Press, November 30, 2020, https://apnews.com/press-release/business-wire/business-government-business-and-finance-coronavirus-pandemic-oil-and-gas-transportation-energy-industry-0810aa8611ca415a92fe3df728bdff72.

8 Brady Dennis and Juliet Eilperin, "Biden Plans to Cut Emissions at Least in Half by 2030," *Washington Post*, April 20, 2021, https://www.washingtonpost.com/climate-environment/2021/04/20/biden-climate-change/.

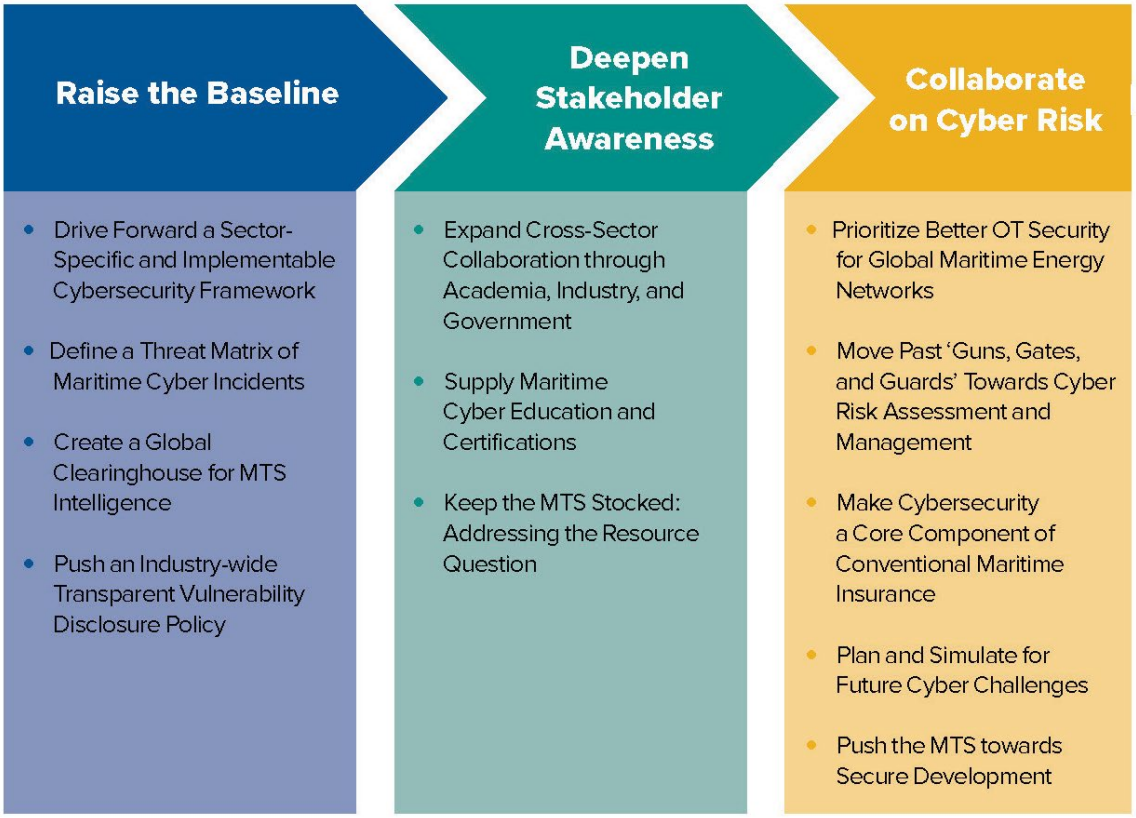
9 "Maritime Cyber Attacks Increase by 900% in Three Years," *Hellenic Shipping News*, July 21, 2020, https://www.hellenicshippingnews.com/maritime-cyber-attacks-increase-by-900-in-three-years/.

Moreover, regulation of the MTS is often indirect because of the interwoven nature of ship management, where many different states and entities might own, lease, sail, register, and crew one ship.

To address this complexity and help stakeholders address the cyber risks impacting the MTS, this report examines three key life cycles—the life of a ship, of a piece of cargo, and of the daily operations of a port—to reveal patterns of threats and vulnerabilities. These life cycles help shed light on a globe-spanning cast of characters. Each life cycle highlights areas of concentrated risk and points of leverage against which policy makers and practitioners can collaborate to take action.

Building on this analysis, the report offers twelve recommendations sequenced as first, next, and later. The first set of recommendations includes six matters to be addressed promptly to secure the MTS. These recommendations need to be prioritized for action because they build directly upon mature preexisting relationships, partnerships, and functions to address key drivers of systemic cyber risk in the MTS. Cybersecurity guidelines and standards fall into this category. Work by the National Institute of Standards and Technology (NIST) to develop a framework profile for liquefied natural gas (LNG) operators in the maritime domain demonstrates this maturity and presents a jumping-off point to address the problem of lacking cybersecurity guidelines and standards for the MTS more holistically. The need and willingness across the MTS to improve existing cybersecurity postures are evident, with many differentiated bodies releasing their own guidelines over the last decade and the NMCP outlining it as a key priority going forward.

The next category of recommendations looks to address several areas of concentrated risk in the MTS. However, these actions are built upon points of leverage that are of varying or inconstant levels of maturity. One of the key recommendations in this section seeks to address the issue of insecure system design: how can vendors design systems to be robust in the face of attacks and fail more gracefully? In recent years, and even more so after the Sunburst campaign, there has been a marked increase in initiatives pushing for secure-by-design policies across many sectors, and acquisition bodies are often responsible for enforcing these initiatives. However, the prospect of applying comparable programs to the MTS is wickedly challenging—and although the end result would be extremely beneficial to the ecosystem, it may ruffle some feathers. Many maritime vendors have been producing the same types of systems for decades and may oppose new, mandatory security controls and design requirements. The commercial MTS vendor community, like the MTS itself, is inherently international, requiring standards or design requirements that are aggressively globalized.



Finally, the report makes two later recommendations regarding vulnerability disclosure programs and cyber insurance. Both present differentiated but equally problematic paths toward influencing better cybersecurity in the MTS—chiefly because of misaligned incentives. Vulnerability disclosure programs and mandatory disclosure windows are currently utilized to help better secure ecosystems and specific systems in other industries. A ninety-day mandatory disclosure policy is commonplace in the technology space. However, the quick timelines that often come with these programs can be challenging for maritime actors. Often, a single operator can have hundreds of ships around the globe, and some or many of them may need to address an identified vulnerability: yet no two of the operator's ships may contain the exact same systems, and consistent access to high-speed Internet zones may be hard to come by. Compared with some other critical infrastructure sectors that can push for a so-called rapid-patch approach, these windows can be unrealistic in the MTS. Implementing an industry-wide mandatory disclosure policy would be a way to draw attention to the problem; however, there would be significant pushback and legitimate questions about whether this policy is realistic.

All twelve of the recommendations put forward by this report are important steps to improve the overall cybersecurity posture of the MTS. By prioritizing actions that are built upon more mature players, protocols, and relationships, this report aims to tackle low-hanging fruit before transitioning to challenging but no less important problems. By following this road map, hopefully, the MTS can work to raise the baseline for cybersecurity and better protect its actors from systemic cyber threats.

2. Introduction

Oceans have long been the lifeblood of international trade and commerce. For more than five thousand years, humans have used rivers, lakes, and the seas to move goods from place to place quickly and efficiently.[10] As civilizations continued to expand and better understand the strategic advantages of maritime trade, this usage accelerated. Initially logs bound together with rope, watercraft evolved into small, carved, wooden vessels. Before long, the first major trade routes began to surface—and the global maritime transportation network was well on its way.

Today, maritime transportation contributes to one-quarter of US GDP, or some $5.4 trillion.[11] No global supply chain is independent of maritime transport, and most, in fact, are existentially dependent on it. Outside the United States, the sea and ports worldwide moved around 80 percent of global trade by volume and over 70 percent of global trade by value.[12] Global maritime trade continues to gather momentum; in 2018, the industry expanded by 4 percent globally—the fastest growth in five years.[13]

The maritime transportation sector also is crucial for the success of other critical infrastructure sectors —specifically, the security of global energy systems. In 2016, more than 61 percent of the world's total petroleum and other liquid energy supply was moved through sea-based trade.[14] Maritime shipping as a form of transportation is essential for bulk transport of these raw materials due to the sheer volume of goods that must be moved and the competitive price point the MTS offers.[15] Maritime trade is essential for supplying fuel to the global economy.

A critical part of the United States' national security is the ability to project power across the oceans; the shipping industry is a crucial cog of this wheel. Sealift—the ability for large-scale transportation of troops, supplies, and equipment by sea—is the basis of US military power projection, handling more than 90 percent of the US Department of Defense's (DOD) wartime transportation requirements.[16] Sealift is the largest provider of strategic mobility, a driver of economic prosperity during wartime, and a key contributor to the US military's global operating model. Sealift has manifested in variety of ways, including shipping essential supplies such as oil and natural gas (ONG) to the Middle East in support of Operation Iraqi Freedom,[17] or providing humanitarian assistance to the Philippines after brutal natural disasters, such as Typhoon Haiyan.[18] The central role of sealift in enabling a diverse set of global operations—and the need to use maritime transportation to enable agile and strategic activity below the level of armed conflic, such as freedom of navigation operations, makes maritime security essential to US national security.

The Merchant Marine Act of 1920—better known as the Jones Act—further defines the relationship between the MTS and national security.[19] Signed into law just after World War I, the Jones Act seeks to promote and maintain the US merchant fleet to ensure that the country will have sufficient merchant sealift capacity in the event of a conflict or an incident requiring the transport of large volumes of personnel and materiel. Among other provisions, it stipulates that any vessels transporting passengers or goods—even liquefied natural gas (LNG)—between US ports must be built, owned, flagged, and crewed by US citizens or permanent residents. A century since the Jones Act's enactment, there are fewer than two hundred vessels that fulfill the statute's criteria,[20] many of which rely on subsidies from the government to maintain that capacity. Despite being one of the largest

10 "The History of the Maritime Industry," North American Marine Environment Protection Association, August 8, 2018, https://namepa.net/wp-content/uploads/2018/08/Lesson-3-The-History-of-the-Maritime-Industry.pdf.

11 Dan Ronan, "Ports, Shipping Industry Responsible for 26% of US GDP, Study Says," *Transport Topics*, April 10, 2019, https://www.ttnews.com/articles/ports-shipping-industry-responsible-26-us-gdp-study-says.

12 "Review of Maritime Transport 2018," UNCTAD.

13 "Review of Maritime Transport 2018," UNCTAD.

14 Business Wire press release, "Global Marine Fuel Market (2020 to 2025)."

15 Business Wire press release, "Global Marine Fuel Market (2020 to 2025)."

16 Sinclair Harris et al., "Sealift: The Foundation of US Military Power Projection," Logistics Management Institute (LMI) blog, May 21, 2020, https://www.lmi.org/blog/sealift-foundation-us-military-power-projection.

17 "Maritime Industry Still Important Facet of National Security," *Federal Drive Time with Tom Temin* (eponymous podcast with guest Brian Clark, a senior fellow), Federal News Network, March 31, 2020, https://federalnewsnetwork.com/workforce/2020/03/maritime-industry-still-important-facet-of-national-security/.

18 "Uptempo: The United States and Natural Disasters in the Pacific," New America, accessed August 5, 2021, https://www.newamerica.org/resource-security/reports/uptempo-united-states-and-natural-disasters/part-ii-military-humanitarian-and-disaster-relief-response-capacity-in-the-indo-pacific-region/.

19 "Jones Act," Legal Information Institute, Cornell Law School website, https://www.law.cornell.edu/wex/jones_act.

20 "Number and Size of the US Flag Merchant Fleet and Its Share of the World Fleet," US Bureau of Transportation Statistics, https://www.bts.gov/content/number-and-size-us-flag-merchant-fleet-and-its-share-world-fleet.

producers of natural gas, the United States is restricted by the Jones Act from shipping its own LNG to domestic ports on noncompliant vessels.

More broadly, maritime trade also plays a key role on the global geopolitical stage for allies and potential adversaries. The United States is dependent on the ability to import goods from its allies via maritime transport: around 90 percent of US total imports arrive by sea. China, a near-peer rival of the United States, is acutely dependent on imports of oil and key resources such as iron to fuel its growing economy—goods that are almost exclusively transported through maritime trade routes.[21] Maritime security is of vital interest to China, as the geography of the the Asia-Pacific region and, specifically, the strategically significant straits of Malacca and Singapore represent some of the most critical choke points and active trade routes in the the world[22]—and global maritime traffic has increasingly concentrated on these geostrategic choke points.

All of these factors have driven industry players to boost efficiency, automation, and remote management, in a word, more technology. The result however is widespread adoption of software and hardware without adequate corresponding management of the growing specter of cyber risk.

2.1. COMPLEXITY BEGETS INSECURITY

Much like many other critical infrastructure industries, operational efficiency and profit drive maritime transportation. That drive has caused a shift toward an even more complex environment—and complexity begets insecurity. As the size of the global economy and its reliance on maritime activity have accelerated, the maritime transportation sector has had to scale up its operations. Over the last fifty years, the size and capacity of cargo ships have increased 1,500 percent.[23] In many ways, this dramatic scale-up has been essential for the industry. It has allowed for an exponential increase in sea trade and has driven prices down internationally. This rapid increase in size, however, has resulted in ships, and the MTS more broadly, becoming more complex.

The MTS is not monolithic. It's a "system of systems" composed of ships and ports, but also the shipping lines, manufacturers, intermodal transport operators, cargo and passenger handlers, vessel traffic control, and maritime administrators. Each of these is itself a system of systems with complex internal and external dependencies. While all ports have similarities, they vary in their ownership and tenant models, cargo- and passenger-handling capabilities, mix of civilian and military vessels, jurisdictional authorities, and more. Similarly, all ships have some common functions, but are fundamentally different in areas such as operation, cargo and passenger capabilities, and crew requirements. Applying regulations to vessels is often complicated by the fact that one's country of registration, ownership, and management might all be different, thus often requiring the coordination of several countries when adjudicating an incident.

Cybersecurity needs to be implemented and practiced by people engaged in all maritime activities—not just IT experts. The users of the MTS are a mixed lot: they work for a wide variety of organizations, play myriad roles, and have varied professional backgrounds and experiences. A given body of water might see any combination of commercial, law enforcement/public safety, military, cargo, passenger, recreational, maintenance, and other types of boats—not to mention offshore drilling or wind platforms, weather and navigation buoys, and sea-based communication platforms.

For years, the maritime sector developed and deployed unique software and hardware, inherently limiting their connectivity and risk exposure.[24] However, the interconnected and data-rich world of the twenty-first century has provided ship and port owners and operators with an opportunity to integrate more ubiquitous IT systems with OT ones. These changes have led to increased automation, digitalization, levels of operational efficiency, and of course, better margins for owners and operators. Despite the MTS's increasing deployment of OT and interconnected technology, from ships to rigs to ports, the sector has not proportionally increased its focus on cybersecurity.

Existing cybersecurity efforts in the MTS prove that it is tough to securely design, develop, and operate a fully connected environment—and even more so when these environments look different on a ship-to-ship and port-to-port basis. The MTS's increased reliance on converging OT and IT systems has introduced new vulnerabilities and expanded the attack surface in the maritime environment—yet the focus and resources devoted to combatting these new threats still largely lags this development. In the integrated MTS, cybersecurity is only as good as the weakest link. It is critical that all links in the MTS logistical chain collaborate

21 Ishaan Tharoor, "What the *Ever Given* Saga Taught Us about the World," Analysis, *Washington Post*, March 30, 2021, https://www.washingtonpost.com/world/2021/03/30/suez-canal-ever-given-lessons/.

22 Lejla Villar and Mason Hamilton, "Maritime Choke Points Are Critical to Global Energy Security," US Energy Information Administration, August 1, 2017, https://www.eia.gov/todayinenergy/detail.php?id=32292.

23 Villar and Hamilton, "Maritime Choke Points."

24 Trey Herr, Will Loomis, and Xavier Bellekens, "Trouble Underway: Seven Perspectives on Maritime Cybersecurity," Atlantic Council blog, March 01, 2021, https://www.atlanticcouncil.org/blogs/new-atlanticist/trouble-underway-seven-perspectives-on-maritime-cybersecurity/.

in establishing robust programs, properly training personnel, and maintaining the operational efficiency necessary for all parts to work as one.[25] However, this is easier said than done.

The consequences of this disconnect—the shortfall in cybersecurity investment compared to the increase in automation and digitization—have become increasingly clear in recent years. This often manifests itself similarly to other industries. Ransomware and phishing, two of the more common tactics and means of compromise globally, exist extensively throughout the MTS. In fact, all four of the world's largest maritime shipping companies—A. P. Moller-Maersk (Maersk, as it is known, is part of the A. P. Moller Group), China Ocean Shipping Company (COSCO) Group, and Mediterranean Shipping Company (MSC)—have been hit by significant cyberattacks since 2017.[26] Maersk, whose business operation systems were ravaged when the NotPetya malware spread from an infected Ukrainian tax-preparation software called MeDoc, spent more than $300 million to return to full operations after ten days of repair and remediation.[27] A reported 400-percent increase in maritime cyberattacks during 2020, along with a 900-percent increase in attacks targeting ships and port systems over the prior three years, point to a maritime industry in the crosshairs of malicious cyber actors. Despite this, the industry and its regulators have only slowly begun to move toward meaningful and systemic change.

Given the complexity and segmented ownership of the organizations comprising the MTS, as well as the range of threats, there is no single authority or cybersecurity model that easily applies to the entire industry. A more modular approach is needed to take a collective understanding of vulnerabilities and threats, and segment the MTS into individual systems that can support one another and/or leverage gains in other systems, and be addressed by policy makers. The approach ultimately must be holistic; even if every component of the MTS was cyber secure, the interconnection of the subsystems might not result in a secure whole. A better understanding of the cybersecurity threat landscape, coupled with a segmented view of MTS infrastructure, will be necessary to build a secure maritime domain. This approach will allow developers, policy makers, owners, and regulators to match the best policy levers with particular maritime systems, and achieve better management of cyber risk across the entire MTS.

2.2. THREATS

The elements, pirates, and rival powers have challenged the maritime shipping industry for thousands of years. As the industry expands in size and integrates new technologies for added efficiency, the volume of potential threats,[28] and the consequences of potential disruption increase exponentially.

In addition to the implementation of new and insecure technology, in the last several years new problems and worsening effects have challenged the maritime industry in different ways. In early 2021, a Maersk vessel lost 260 containers overboard—about 2 percent of its cargo—when the ship lost propulsion for less than four minutes in heavy seas.[29] This was not an isolated incident; both MSC and NYK Shipmanagement (NYKSM) have each had significant and comparable incidents since late-2020.[30] Over the last decade, the World Shipping Council estimated that an average of 1,382 containers have been lost overboard annually.[31] While not all of these losses are linked to cyber incidents, they illustrate how much risk exists in the ecosystem, and how the increased scale and complexity of the MTS have given rise to new concerns.

The COVID-19 pandemic is evidence of the effects that a massive disruption can inflict on the MTS. The pandemic challenged the maritime industry with port closures, a new and shifting demand landscape, significant supply-chain disruptions, and operational questions around health and safety. As a result, for the first time in decades, global maritime trade actually dropped 4.1 percent in 2020.[32] No doubt, the pandemic also will have long-term effects on the industry that are hitherto impossible to quantify. COVID-19 forced

25 Herr, Loomis, and Bellekens, "Trouble Underway."

26 Catalin Cimpanu, "All Four of the World's Largest Shipping Companies Have Now Been Hit by Cyberattacks," *ZDNet*, September 28, 2020, https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/.

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

28 "Maritime Industry Sees 400% Increase," *Security*.

29 "Updated: Maersk Boxship Losses [*sic*] 260 Container [*sic*] Overboard during Blackout," *Maritime Executive*, February 17, 2021, https://www.maritime-executive.com/article/blackout-on-maersk-boxship-causes-another-significant-container-loss.

30 Mike Schuler, "More Containers Lost in the Pacific as 41 Go Overboard from MSC Ship," *gCaptain* website, February 2, 2021, https://gcaptain.com/msc-boxship-loses-containers-in-the-pacific/; and Kim Link-Wills, "Storm-beaten ONE Apus Berths in Japan," *American Shipper*, a FreightWaves unit, December 8, 2020, https://www.freightwaves.com/news/storm-beaten-one-apus-berths-in-japan.

31 World Shipping Council, "Containers Lost at Sea: 2020 Update," undated PDF, https://www.worldshipping.org/Containers_Lost_at_Sea_-_2020_Update_FINAL_.pdf.

32 "COVID-19 Cuts Global Maritime Trade, Transforms Industry," UNCTAD, November 12, 2020, https://unctad.org/news/covid-19-cuts-global-maritime-trade-transforms-industry.

states to think differently about their international relationships and trading patterns.[33] The economic and security consequences of such a large-scale disruption shocked many—and proved how unprepared the MTS is for such systemic challenges.

The most recent and probably most notable single-event example of an MTS-wide disruption occurred when *Ever Given*, one of the largest commercial container ships in the world, got stuck shortly after entering the Suez Canal in March 2021, blocking through traffic on one of the world's busiest waterways. The vessel, at 1,300 feet (400 meters) and nearly 221,000 gross tons, was stuck for more than six days and took several days of work from one of the world's best salvage teams, a fortuitous high tide, and a dash of luck to unwedge. Although the cause of the incident is believed to be a combination of heavy winds, the ship's speed, and the vessel's rudder size/alignment rather than a cyber attack,[34] the mishap caused global economic disruption. With 13 percent of global trade passing through it every year, the narrow Suez Canal is one of the most strategically important choke points in the world.[35] The resultant blockade of Suez Canal traffic held up $9.6 billion in goods.[36] Once unstuck, the price to "refloat" the ship landed at $900 million, to be followed by a dispute over financial damages that ended in the seizure of *Ever Given* for nearly four months by Egyptian authorities.[37]

The *Ever Given* incident illustrates the scale of disruption that a cyber incident could have on global shipping, especially in geostrategic choke points. It also exemplifies the complexity and interconnectedness of the global maritime system. *Ever Given* was owned by a company in Japan, operated by a container shipping firm based in Taiwan, managed by a German company, registered in Panama, and crewed by twenty-five Indian nationals.[38] The complex, interconnected, and multinational nature of the MTS makes coordination challenging and finger pointing around incidents common—but also provides the industry with a unique opportunity to leverage systemic and global change if handled correctly.

There are precedents for high-consequence cyber events causing disruption on the MTS, including in the United States. In November 2020, the Port of Kennewick was hit by sophisticated ransomware attack that forced operators to rebuild the Washington state port's digital files from offline backups.[39] This was not an isolated incident, but emblematic of a larger trend.[40]

The cyber-threat landscape in the MTS is similar to that of other critical infrastructure sectors. Global Positioning System (GPS) and Automatic Identification System (AIS) jamming and spoofing, attacks on less-than-secure OT and industrial control-system (ICS) devices, human targets, myriad shipboard information and communications technology (ICT) systems, are just some of the vectors that adversaries can and will use to attack the MTS. Ransomware, software supply-chain attacks, and social engineering are a few common tactics, techniques, and procedures (TTP) that have been used against the MTS. Potential targets and victims throughout the MTS include ships, ports, passenger and cargo shipping lines, shipbuilders and maritime manufacturers, and others. It is a complex and extraordinarily dynamic ecosystem that is difficult to defend. Cyberattacks represent an existential threat to the contemporary maritime industry, the smooth operation of which underpins modern society.

2.3. ATTACKERS AS DIVERSE AS THE MTS: PIRATES TO PWNERS

The MTS's vulnerability to cyberattacks and its significance to US national security and economic stability have drawn from the woodwork an array of adversaries intent upon wreaking harm on the ecosystem.

Just as the MTS is not monolithic, neither are those posing a threat to it. There is no single profile of a threat actor and motivation for attacking maritime cyber systems. Sun Tzu's well-known saying about knowing thy enemy applies here: "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer

33 Marcus Baker, "The Pandemic Is a Top Maritime Industry Issue—But It's Not the Only One," *Brink*, a news platform of Marsh McLennan Advantage, October 12, 2020, https://www.brinknews.com/coronavirus-pandemic-becomes-a-top-maritime-industry-issue-but-its-not-the-only-one/.

34 Mia Jankowicz, "Here Are the Main Theories of How the *Ever Given* Got Stuck in the Suez Canal," *Business Insider*, March 30, 2021, https://www.businessinsider.com/how-ever-given-got-stuck-in-suez-canal-main-theories-2021-3.

35 "SCZone Head: 13% of World Trade Passes through Suez Canal," *Hellenic Shipping News*, June 24, 2019, https://www.hellenicshippingnews.com/sczone-head-13-of-world-trade-passes-through-suez-canal/.

36 Justin Harper, "Suez Blockage Is Holding Up $9.6bn of Goods a Day," BBC News, March 26, 2021, https://www.bbc.com/news/business-56533250.

37 Mostafa Salem, Mai Nishiyama, and Pamela Boykoff, "Egypt Impounds *Ever Given* Ship over $900 Million Suez Canal Compensation Bill," CNN Business, April 14, 2021, https://www.cnn.com/2021/04/13/business/ever-given-seized-compensation-bill-intl/index.html.

38 Tharoor, "What the *Ever Given* Saga Taught Us," Analysis.

39 Martyn Wingrove, "Cyber Attack Shuts Down US Port Servers," *Riviera* news hub, Riveria Maritime Media, November 23, 2020, https://www.rivieramm.com/news-content-hub/news-content-hub/cyber-attack-shuts-down-us-port-servers-61955.

40 Nicole Sadek, "Shipping Companies Confront Cyber Crooks as Economies Reopen," Bloomberg Government (news and analysis service), June 29, 2021, https://about.bgov.com/news/shipping-companies-confront-cyber-crooks-as-economies-reopen/.

a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." Understanding where your risk is concentrated and who may look to exploit that risk are essential steps to securing an organization's systems.

Attackers in cyberspace generally fall within the following categories based largely on intent.[41]

1. **Cybercriminals:** Like criminals in the physical domain, cybercriminals are after financial or other tangible rewards; they are not ideologues, they want the cash. Cybercrime costs the global economy more than $1 trillion annually.[42] Cybercriminals in the MTS engage in cyberfraud and are behind most ransomware campaigns.

2. **Cyber activists/hacktivists:** Philosophy, politics, social movements, and other nonmonetary goals motivate this group of threat actors. Typical tactics of hacktivists include defacing websites, launching protests on social media, and conducting acts of cyber vandalism; while often criminal in nature, the intent is rarely financial.

3. **Terrorists:** The use of cybersecurity capabilities by a traditional terrorist actor could mirror an act of terrorism in real space—a violent criminal action, meant to intimidate or cause fear—and be motivated by political aims. This fear could directly, or indirectly, yield disruption with significant economics effects. Terrorrist groups also often engage in cyberattacks with financial motivations to fund other operations and help support recruitment.

4. **State-sponsored entities:** These actors often report to or receive support from nations or states. Acts of financial, industrial, political, and diplomatic espionage in cyberspace are the most common objectives for this type of entity. Intellectual property (IP) theft, in particular, costs the global economy more than $2 trillion annually by some estimates.[43]

5. **State actors:** Such actors have the resources and capabilities to conduct nuanced and sophisticated cyber operations. Although the most prominent state actors targeting the MTS are Russia and China, both Iran and North Korea have proven capable of attacking numerous industrial sectors internationally. These operations normally work to advance strategic goals. There is no international consensus on a definition of "an act of war" in cyberspace and, therefore, it is unclear how defense treaties in traditional spaces influence hostile activities in cyberspace.

While an understanding of the distinctions among threat actors can be useful in considering how to protect specific systems, a strict categorization of any given cyberattack is often difficult because the lines differentiating these actors blur during any dynamic event. Attribution is often a challenging and lengthy process, and results can sometimes be tentative at best. Many criminal organizations in cyberspace, for example, have nation-state sponsors yet their actions are not considered state-sponsored.

Attackers have their own motivations, levels of capability, technological and financial resources, opportunities, time frames, and intents. The primary threat actors that have demonstrated a high capacity and willingness to conduct operations against the MTS and related critical infrastructure sectors fall within two categories: cybercriminals and state-sponsored actors. There are thin boundaries between these categories, given that some state-sponsored groups also operate within well-known cybercriminal networks.

The main focus of cybercriminals is most often monetary gain. They target well-known organizations with large attack surfaces, prey on employees' lack of cyber awareness, and aim for large monetary rewards. To accomplish these ends, ransomware has become one of the most common and public forms of cyberattacks against MTS targets. Ransomware is used to paralyze a victim organization by encrypting its data and requesting a ransom, often to be paid into a pseudonymous cryptocurrency wallet. Most ransomware attacks are conducted by criminal organizations for their own profit, or to fund criminal and terrorist activities in conventional space. Some other monetary motivations include reselling access to the infrastructure, information obtained, or compromised computers on the darknet, a network using the Internet that requires permission or special software.

Cyberespionage operations targeting the maritime community also are common, primarily in the form of intelligence gathering and Internet Protocol (IP) theft. Cyberespionage represents a middle ground of activity that can be valuable for both criminals and state actors. In March 2019, for example, Chinese state-sponsored hackers reportedly targeted

41 Gary C. Kessler and Steven D. Shepard, "Maritime Cybersecurity: A Guide for Leaders and Managers" (self-pub., 2020), 49-50.

42 Jai Vijayan, "Global Cybercrime Losses Cross $1 Trillion Mark," *Dark Reading* news site, December 9, 2020, https://www.darkreading.com/attacks-breaches/global-cybercrime-losses-cross-$1-trillion-mark/d/d-id/1339655.

43 Bruce Berman, "Cost and Sources of Global Intellectual Property Theft Include China and the U.S.," *IP CloseUp*, Close Up Media, June 23, 2020, https://ipcloseup.com/2020/07/23/cost-and-sources-of-global-intellectual-property-theft-include-china-and-the-u-s/.

universities around the world, as well as the US Navy and industry partners, in order to steal maritime technology.[44] China also has an ownership and/or operational presence at dozens of major ports around the world, providing a wide capability for information gathering on ports, vessels, and cargoes. Obtaining this type of access to MTS infrastructure can provide information of strategic significance regarding MTS cyber-physical security, information-system vulnerabilities, and operational information. Furthermore, adversaries may consider breaching a network using zero-day attacks to maintain persistent access to MTS networks to affect or influence the infrastructure operations at the right time.[45]

More sophisticated, state-sponsored attacks are just starting to find their way into the MTS, with incidents such as the May 2020 cyberattack by Israel on Iran's Shahid Rajaee port in Bandar Abbas in response to Iran's cyberattack on Israel's water-supply system the previous month.[46] Directed spoofing and jamming attacks on global positioning, navigation, and timing (PNT) systems by Russia, China, Iran, and North Korea are additional threats affecting the MTS as well as other transportation sectors.

2.4. FRAMING THE CHALLENGE

It is imperative to establish at the outset that there is no silver bullet for maritime cybersecurity. A history of old shipboard technology has been retrofitted to an era of interconnectivity, which has created a fractured and vulnerable maritime environment.

This report is intended to deliver a more complete and operational plan to better protect the MTS by focusing on building upon, broadening, and deepening the priorities put forward by the NMCP. The US government took an important first step in December 2020 when it released the National Maritime Cybersecurity Plan.[47] The plan aims to "buy down the potential catastrophic risks to national security and economic prosperity caused by MTS operators' increasing reliance on IT and OT, while still promoting maritime commerce efficiency and reliability." To achieve this goal, the plan focuses on three key principles: risks and standards, information and intelligence sharing, and creating a maritime cybersecurity workforce. The plan represents a significant step in the right direction and calls attention to many of the critical risks outlined in this report. However, it lacks specificity on how to implement these three principles.

This report started by highlighting both the significance of the MTS and some of the most common and consequential threats to the MTS. Now it pivots to discuss major drivers of risk to the MTS and three maritime life cycles—ships, ports, and cargo—and the key programs, vulnerabilities, and stakeholders in each. These sections are explicitly intended to extend the NMCP and identify areas of risk and potential progress for policy makers and industry. The final section builds on the points of leverage identified in these three life cycles and offers specific recommendations to the United States, US allies, and the private sector to cooperatively reduce and better manage the system's cybersecurity risks.

44 Emily Price, "Chinese Hackers Targeted 27 Universities to Steal Maritime Research, Report Finds," *Fortune*, March 5, 2019, https://fortune.com/2019/03/05/chinese-hackers-targeted-27-universities-to-steal-maritime-research-report-finds/.

45 To the reader, the term zero-day (also known as 0-day) refers to cyberattacks on a software vulnerability before developers find and fix it.

46 Ronen Bergman and David M. Halbfinger, "Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks," *New York Times*, May 19, 2020, https://www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html.

47 *National Maritime Cybersecurity Plan to the National Strategy for Maritime Security*, Office of the White House, 2020.

3. A "System of Systems": Understanding the MTS

The MTS is a markedly complex "system of systems." This report segments the MTS into three discrete systems—ships, ports, and cargo—each with its own life cycle. In this context, a life cycle is an analysis of the progression of a specific unit or system within the maritime transportation system. This section discusses each of these system's interactions, processes, systems, and vulnerabilities. These three systems do not capture the entirety of the MTS, but they embody the entities most central to the sector and its security. This report seeks to highlight areas of risk and leverage for policy makers and the industry. The goal of this section is to illustrate the complexity and diversity of these core systems and expose potential points of leverage for policy change in each. Not all actors, problems, and processes fall neatly into these systems, while others are elements in every system.

Before focusing on these life cycles, it is important to identify where the sources of systemic cyber risk exist in the MTS. Although these risks manifest themselves in different ways for the distinct subsystems of the MTS, they are all proven concentrations of cyber risk that one must consider when trying to protect the MTS from cyber threats.

In the late 2000s, the public and private sectors quickly adapted security postures to address the threat posed by modern-day piracy. Years after addressing the threat, the security measures implemented then remain permanent fixtures of ships. This example demonstrates the maritime industry's adeptness in reactively responding to crises, though it strongly contrasts with the industry's lack of proactive behavior in addressing emerging cyber threats. There is a disconnect between the MTS and the myriad potential cybersecurity threats it faces from a gamut of criminal enterprises and states. Every misconfigured device or user-restrictive system creates a new vulnerability that opportunistic threat actors can exploit. This section aims to highlight some of the most common and consequential sources of systemic risks in the MTS.

There are two key categories of systemic risk for the MTS: human risk and systems risk. The intent of this section is to specifically highlight that vulnerabilities in technology are an important risk factor in the MTS, but the human element—and the inherent risk associated with humans working with complex and challenging-to-understand technical systems—is just as critical.

3.1 HUMAN CYBER RISK

It is a common mantra in security that humans are the weakest link in the defensive chain. However, humans are also essential to any solution. A large number of cybersecurity papers,[48] conference presentations,[49] and corporate studies focus on this dichotomy—so much so that the human weak link is sometimes accepted as an unalterable fact.[50]

The cliché clearly implies that the *user* is the weakest link in cybersecurity with no mention of the *designer* of the critical IT and OT systems. This seems to suggest that there is perfect information security—computers with locked down operating systems (OS), resilient applications software, secure communications protocols, and strong encryption—that can withstand any attack, until a human user enters the picture. This is not an accurate description of computer systems. No OS is completely secure, because no developer can patch all known vulnerabilities during every patch cycle, much less those yet unknown; hence the large arsenal of zero-day exploits in the wild just waiting to be launched. Software undergoes a frequent update and patch cycle. This makes the uniform distribution of the latest "up-to-date version" difficult within a large enterprise system. A communications protocol might be secure on paper, but then suffer from flaws in implementation. Indeed, many of these depend upon encryption schemes that are mathematically solid, but then weakened due to flaws in the software implementation or mismanaged keys. These vulnerabilities are not user created; they are intrinsic to any system designed and run by humans.

This becomes even more challenging with a complex ecosystem like the MTS. Ships and ports are often operating with rotating crews that may not be fully familiar with their vessels, systems, and established cyber-hygiene practices. Furthermore, crews may have varying levels of cyber literacy. A lack of digital culture and cyber literacy may benefit

48 Lance Spitzner, "This Is Why the Human Is the Weakest Link," Information Security Training, SANS Institute blog, January 1, 2021, https://www.sans.org/blog/this-is-why-the-human-is-the-weakest-link/.

49 Alan Shimel, "CISO Talk: The Human Side of Cybersecurity," Security Boulevard, a unit of MediaOps, February 17, 2021, https://securityboulevard.com/2021/02/ciso-talk-the-human-side-of-cybersecurity/.

50 Bob Kress, "Why Humans Are Still Security's Weakest Link," Accenture blog, August 31, 2020, https://www.accenture.com/us-en/blogs/security/humans-still-securitys-weakest-link.

an attacker's ability to gain information on a vessel and its systems or disrupt the vessel's operations. More than anything, there is a critical need in the MTS to better understand the problems facing the sector. The easiest way to do this is more cybersecurity training, education, and certification for the MTS and its operators.

For the purposes of this report, human cyber risk in the MTS divides into four discrete categories: social engineering, lack of cyber hygiene, unauthorized access, and overcomplicated technology.

Social Engineering

As discussed above, humans are the most valuable, but also the most vulnerable aspect in maritime cybersecurity, because they are the ones operating critical systems.[51] Social engineering—or the manipulation of people—is one of the most common cyberattack vectors. Social-engineering methods include baiting, email, voicemail, and SMS phishing (and its variants), malicious email attachments, and pretexting, as well as simple deception.[52] These techniques can be used by attackers to manipulate people into letting them gain access to personal computers of crew members or operators in the hopes of infecting maritime systems.

Imagine an oil tanker chosen as a target by a hacking group. In today's society, writes a chief officer working on commercial vessels, "information regarding the vessel's static and dynamic (course/speed/position) data, crew composition, type and quantity of cargo, destination, captain's name, and other items of interest could be collected from the web."[53] Attackers could search and exploit the social media networks of crew members, preferably the targeted vessel's bridge team members, for additional information and deploy a spear-phishing campaign to harvest administrator-level credentials. Social media networks and websites focused on professional groups and employment make these tasks easier. With that access, the tanker's network would be within relatively easy grasp of the hacking group.

Ships are direct targets of many of these attacks. In May 2019, the United States Coast Guard (USCG) issued a Marine Safety Information Bulletin (MSIB) specifically warning commercial vessels about targeted cyberattacks where malicious actors, using email addresses that appeared to be from a Port State Control authority, sought sensitive information such as crew members' names, personally identifiable information (PII) and protected health information (PHI), many times under the guise of COVID-19 management.[54]

Holland America Line and Princess Cruises—both subsidiaries of Carnival Corporation—were victimized by a phishing campaign in May 2019, although it was not announced until March 2020.[55] The adversary sent phishing emails to employees to gain access to employee email accounts, where it was able to reap employee and customer PII, including names, Social Security numbers, other government identification numbers, passport information, credit card and financial information, and PHI, according to the report.

Ships and shipping lines are not the only potential targets. Bunker companies, fuel suppliers, shipping management companies, port operators, shipbuilders, and charterer companies could all be targeted and defrauded via email-based social-engineering attacks.

Lack of Cyber Hygiene

Lack of basic cybersecurity best practices, or cyber hygiene, is a critical driver of risk for the MTS. Ship crew or port operators might not be aware of the risks of downloading files from the Internet, not enabling multifactor identification, clicking on email links, or the lack of anti-virus software and firewalls on their computers. An attacker may attempt to take advantage of a crew's lack of cyber awareness and hygiene by sending phishing emails to its members. Segregation between the crew network and the bridge network may erode during an attack, creating more problems. Anecdotes abound about poor cyber hygiene, including bridge crews implementing differentiated password controls only to post the new passwords on sticky notes. Such insecure practices highlight the challenges within the MTS when it comes to cyber awareness and hygiene.

With such enormous variation in missions and environments, ship and port managers often operate with rotating crews that may not be fully familiar with the port or vessel, its systems, and inherently the cybersecurity measures, or cyber hygiene standards, that accompany them.

51 Oliver Fitton et al., *The Future of Maritime Cyber Security*, Lancaster University, n.d., https://eprints.lancs.ac.uk/id/eprint/72696/1/Cyber_Operations_in_the_Maritime_Environment_v2.0.pdf.

52 "What Is Social Engineering: Attack Techniques and Prevention Methods," Imperva Inc. website, December 29, 2019, https://www.imperva.com/learn/application-security/social-engineering-attack/.

53 Leonid Vashchenko, "Digital Perils: Socially Engineered Attacks in Maritime Cybersecurity," Opinion, *Maritime Executive*, March 5, 2021, https://www.maritime-executive.com/editorials/digital-perils-socially-engineered-attacks-in-maritime-cybersecurity.

54 US Coast Guard, "Cyber Adversaries Targeting Commercial Vessels," May 24, 2019, https://www.dco.uscg.mil/Portals/9/DCO Documents/5p/MSIB/2019/MSIB_004_19.pdf.

55 Megan Leonhardt, "Princess Cruises and Holland America Data Hacks 'Create Extraordinary Levels of Risk'—Here's What to Do If You Were Affected," CNBC, March 5, 2020, https://www.cnbc.com/2020/03/05/how-to-protect-yourself-from-princess-cruise-and-holland-america-data-hack.html.

Poor password practices are legion throughout the ICT-user community, and the maritime sector is no different. In August 2015, a white hat hacker reported on the ability to eavesdrop on Globalstar satellite communications systems that were both unencrypted and employing default passwords; these Internet-connected devices could be found using the Censys or Shodan search engine.[56] In October 2017, another white hat hacker detailed how SAILOR 900 VSAT systems—one of the market leaders for maritime telecommunications—around the world continued to use default passwords that could be found on Censys or Shodan as well.[57] In October 2018, a 19-gigabyte Navionics database, which contains details on more than 260,000 customers, was found unsecured online due to a misconfigured database that had no password.[58] These are just a few examples of how the prevalence of poor cyber hygiene can hamstring efforts for increased cybersecurity in the maritime domain.

Unauthorized Access

Ships and ports are expansive and notoriously difficult to keep protected at all times. With multiple organizations, contractors, and entities working together on each ship and at each port, keeping strict oversight of access control levers can be difficult. This can manifest itself in two main ways. The first is the insider threat. Whether the individual has a personal vendetta or is bowing to manipulation by another actor through blackmail or monetary incentives, insider threats are an important threat vector. An insider attacker with intimate knowledge may be able to physically bypass access controls and restricted parts of buildings containing critical IT and OT systems, either using their own credentials or leveraging their knowledge of the port and its systems. For example, an insider attacker could gain access to a command-and-control room and place key loggers at the back of computers using a simple USB stick,[59] allowing them to retrieve desired information on port systems, including logins and passwords. A 2018 report highlighted at least two instances of abused access to deploy USB thumb drives with malware onto maritime systems.[60] These actions can result in serious, long-term consequences.

The second primary manner of obtaining unauthorized access is through linking secure and essential systems to insecure systems. Wireless networks have become the norm for web surfing and day-to-day operations in many industries across the globe. However, these networks, given their expanded use by the MTS, are attractive targets for attackers to connect to essential systems in a port or on a vessel and potentially cause significant damage.

Overcomplicated Technology

In recent years, the maritime industry has pushed aggressively for technological integration, more automation, and new and improved systems. Although some new systems make sailors' lives easier and more efficient, changes can create significant new security problems. A dearth of qualified technical know-how onboard ships exacerbates technological complexity, but it is not the source of the problem.

In 2019, the USS *John S. McCain* collided with the Liberian-flagged oil tanker *Alnic* MC.[61] After an extensive review of the incident, investigators determined that an overly complicated touch-screen steering system and inadequate training were major contributors to the collision. The *McCain* helmsman said, "There was actually a lot of functions on there that I had no clue what on earth they did." Afterward, a report by the National Transportation Safety Board (NTSB) said, "the design of the *John S. McCain's* touch-screen steering and thrust control system increased the likelihood of the operator errors that led to the collision."[62] This example calls attention to the potential risk of increasingly common overcomplicated technologies in the MTS.

3.2 SYSTEMS CYBER RISK

The MTS is comprosed of heterogeneous, complex, and often legacy systems. Maritime systems are in a constant state of evolution. Assets are highly interconnected, include both stationary (e.g., land-based) and mobile (e.g., shipboard) infrastructures, and, in many cases, remain in almost constant use. Both fixed and mobile infrastructures are interdependent and interlaced. At their core, they are driven by processes and tools such as data flows, OT systems, OT end devices, ICT systems, ICT end devices, cloud infrastructures, networked nodes, communication systems,

56 Patrick Tucker, "Hacker Cracks Satellite Communications Network," *Defense One*, August 6, 2015, https://www.defenseone.com/technology/2015/08/hacker-cracks-satellite-communications-network/118915/.

57 Ken Munro, "OSINT from Ship Satcoms," PenTestPartners blog, October 13, 2017, https://www.pentestpartners.com/security-blog/osint-from-ship-satcoms/.

58 Charlie Osborne, "Garmin's Navionics Exposed Data Belonging to Thousands of Customers," *ZDNet*, October 9, 2018, https://www.zdnet.com/article/garmins-navionics-exposed-data-belonging-to-thousands-of-boat-owners/.

59 Fitton et al., *The Future of Maritime Cyber Security*.

60 Catalin Cimpanu, "Ships Infected with Ransomware, USB Malware, Worms," *ZDNet*, December 12, 2018, https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms/.

61 T. Christian Miller et al., "Collision Course," *ProPublica*, December 20, 2019, https://features.propublica.org/navy-uss-mccain-crash/navy-installed-touch-screen-steering-ten-sailors-paid-with-their-lives/.

62 "Collision between US Navy Destroyer *John S McCain* and Tanker *Alnic MC*, Singapore Strait, 5 Miles Northeast of Horsburgh Lighthouse, August 21, 2017," National Transportation Safety Board, Report Adopted June 19, 2019, https://www.ntsb.gov/investigations/AccidentReports/Reports/MAR1901.pdf.

and safety and security systems. This profusion of systems and components ranges from generic IT and OT devices to more niche elements that are specific to the maritime ecosystem. Out of all these potential attack vectors, four stand out in terms of vulnerability, volume of exploitation, and consequence.

Attacks on OT Systems

The use of OT—where embedded computers directly control hardware—throughout ports and ships enables smart maritime systems. OT also includes supervisory control and data acquisition (SCADA) systems, such as flow computers, transport and transfer systems, and monitoring meters, which play a crucial role in the global transportation of oil and natural gas. The technology to support the evolution to smart maritime systems is readily available and being rapidly implemented in ports around the world.

Cybersecurity protections, however, continue to lag behind the pace of technological innovation and implementation. Although attacks on OT systems are still relatively new, cyberattacks targeting OT systems in the maritime domain have increased by 900 percent in the last three years.[63] Uncovered in 2010, the Stuxnet worm targeted Siemens software that managed programmable logic controllers (PLCs) for centrifuges known for their use in Iranian nuclear research facilities. Upon infection, the controlling software would indicate normal operations on the display panel, all the while instructing the centrifuges to spin at their maximum speed and causing them to self-destruct. Stuxnet was the first highly publicized software attack on hardware. Since then, ICS-specific attack tools have proliferated and are readily available on the Internet.[64] The Stuxnet example also proves how an attacker can exploit a vulnerability in the OT infrastructure or SCADA systems that could lead to financial or human losses.

These effects can become even more drastic within the energy sector. In August 2017, Saudi Aramco and Qatar's RasGas were repeat victims of the 2012 Shamoon virus that crashed 30,000 personal computers and nearly reached into OT networks, with the goal of triggering an explosion.[65] The Triton/Trisis malware, first found in the wild in 2018, specifically targeted OT systems and ICS at a Saudi ONG facility. Attacks at energy facilities have the potential to cause physical effects such as explosions, threatening human life and extensive financial harm. Such an attack at a high-volume port could be devastating.

Attacks on IT Systems

Wireless networks dominate day-to-day operations in many industries across the globe, and problems surrounding IT system vulnerabilities are common knowledge. However, reports assessing the security of the maritime industry indicate that open networks and weak encryption networks using the defunct Wired Equivalent Privacy (WEP), or other weak cryptography algorithms, are still in use for Wi-Fi and Internet of Things (IoT) devices in the maritime domain. Such poor network security could expose essential systems in a port or on a vessel to attackers.

The maritime industry's digital transformation has led to widespread cloud adoption to manage personnel information, enterprise resource planning (ERP), customer relationship management (CRM), and other corporate functions. However, lack of cloud security architecture and strategy may lead to misconfigurations and unprotected application programming interfaces (APIs) that can be exploited by attackers to retrieve and collect key data. The SolarWinds supply-chain attack, publicly disclosed in late 2020, demonstrated the frailties of the software supply chain and the linchpin cloud technologies, as well as the exploitable interconnectedness of a system like the MTS.

Attacks on PNT Systems

Ships rely on numerous ship-to-shore communication systems, geopositioning systems, and navigation systems to operate effectively while underway and when entering and exiting ports. Attackers could jam geopositioning systems and ship-to-shore communications, or spoof the communications to threaten the safe navigation of vessels.[66] These techniques could also be used to gain a tactical advantage in a conflict.

Jamming and spoofing are far from hypothetical. GPS and AIS jamming and spoofing are problems that have been widely documented for many years,[67] and issues related to loss in signal, or even a small positioning error, can be magnified within the relatively confined space of a

63 "Maritime Cyber Attacks Increase By 900%," *Hellenic Shipping News*.

64 Jeffrey Ashcraft, "Monitoring ICS Cyber Operation Tools and Software Exploit Modules to Anticipate Future Threats," FireEye blog, March 23, 2020, https://www.fireeye.com/blog/threat-research/2020/03/monitoring-ics-cyber-operation-tools-and-software-exploit-modules.html.

65 Nicole Perlroth and Clifford Krauss, "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try," *New York Times*, March 15, 2018, https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.

66 Sean McCrystal, "Detecting and Defeating GPS Jamming," *Maritime Executive*, February 16, 2020, https://www.maritime-executive.com/blog/detecting-and-defeating-gps-jamming.

67 "Understanding GPS Spoofing in Shipping: How to Stay Protected," *Safety4Sea*, January 31, 2020, https://safety4sea.com/cm-understanding-gps-spoofing-in-shipping-how-to-stay-protected/.

port, particularly when involving increasingly large cargo and passenger ships. In 2019, the nonprofit Center for Advanced Defense Studies (C4ADS) released a report detailing Russian use of GPS spoofing to achieve a variety of disruptive and strategic objectives.[68] Additionally, AIS is among the most critical systems in the maritime industry, as it allows for the exchange of vessel positioning and information alerts, yet it was shown to be systemically insecure as early as 2013.[69] The potential effects of compromised PNT are significant, as modern ships rely heavily on these satellite- and radio-based systems for navigation.

Ransomware

Although it is not a specifically targeted system like the previous three categories, ransomware represents a threat to all types of systems in the MTS.[70] According to the US Cybersecurity and Infrastructure Security Agency (CISA), ransomware is an "ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption."[71] Ransomware groups force companies to pay a ransom to regain control of their systems and/or to prevent the leakage of large quantities of data.

Ransomware has targeted the maritime industry in the past several years, as it has many other industries globally. The trend began in earnest in 2017, when the NotPetya operation took Maersk (and hundreds of other organziations around the world) offline, as discussed above.[72] In 2018, COSCO's North American subsidiary, COSCO Shipping Lines, was hit by ransomware, shutting down its operations and IT systems for days. In 2019, hackers used the Ryuk ransomware to disrupt the entire IT network of the port, as well as several ICS systems used to transport and monitor cargo, for roughly thirty hours, completely halting operations.[73] 2020 was a wake-up call for the maritime industry about the harms of ransomware, as Carnival, CMA CGM Group, Garmin, Hurtigruten, Port of Kennewick, and Toll Group were all victims of ransomware attacks.[74] The interconnected nature of supply chains and the differentiated actor set in the MTS make the industry especially vulnerable to ransomware and more likely to pay off ransoms in order to avoid sustained disruption of these supply chains. To help mitigate the ransomware threat to the MTS, shipping and logistics companies must improve IT hygiene and email security to harden networks against common ransomware tactics.[75]

3.3 MARITIME LIFE CYCLES

It would be impossible to individually address each subsystem in the MTS in one go. This report focuses on three key subsystems: ships, ports, and cargo. While all ports have similarities, they also are different in terms of their ownership and tenant models, cargo- and passenger-handling capabilities, mix of civilian and military vessels, jurisdictional authorities, and more. Similarly, all ships have some common functions but are different in terms of their intended purpose, operation, design, crew requirements, and regulatory practices, among other things. The life cycle for the transportation of cargo is even more differentiated (as are the key systems relied upon), depending on what type of good is being transported. The approaches to building a cyber defense within the MTS must be as varied as the elemental components within it.

In addition to the different subsystems in the MTS, there also are a wide variety of players that are essential to the operation and security of the global MTS. As with the subsystems, it would be extremely challenging to address all of them; instead, the table below maps their roles and responsibilities. For more information on specific players, please see *Appendix 1*.

The following sections examine three different segments of the MTS—ships, ports, and cargo—to demonstrate the interconnectedness of the system of systems that comprises the MTS. These three subsystems of the MTS are both the most critical

68 "Russian GPS Spoofing Threatens Safety of Navigation, Report Says," Safety4Sea, April 8, 2019, https://safety4sea.com/russian-gps-spoofing-threatens-safety-of-navigation-report-says/.

69 Marco Balduzzi et al., "Hey Captain, Where's Your Ship? Attacking Vessel Tracking Systems for Fun and Profit," Eleventh Annual Hack in the Box (HITB) Security Conference in Aisa, October 2013, http://conference.hitb.org/hitbsecconf2013kul/materials/D1T1%20-%20Marco%20Balduzzi,%20Kyle%20Wilhoit%20Alessandro%20Pasta%20-%20Attacking%20Vessel%20Tracking%20Systems%20for%20Fun%20and%20Profit.pdf.

70 Cimpanu, "All Four of the World's Largest Shipping Companies."

71 "Ransomware Guidance and Resources," Cybersecurity and Infrastructure Security Agency (CISA), accessed May 4, 2021, https://www.cisa.gov/ransomware. CISA is an independent federal agency that is an operational component of the US Department of Homeland Security).

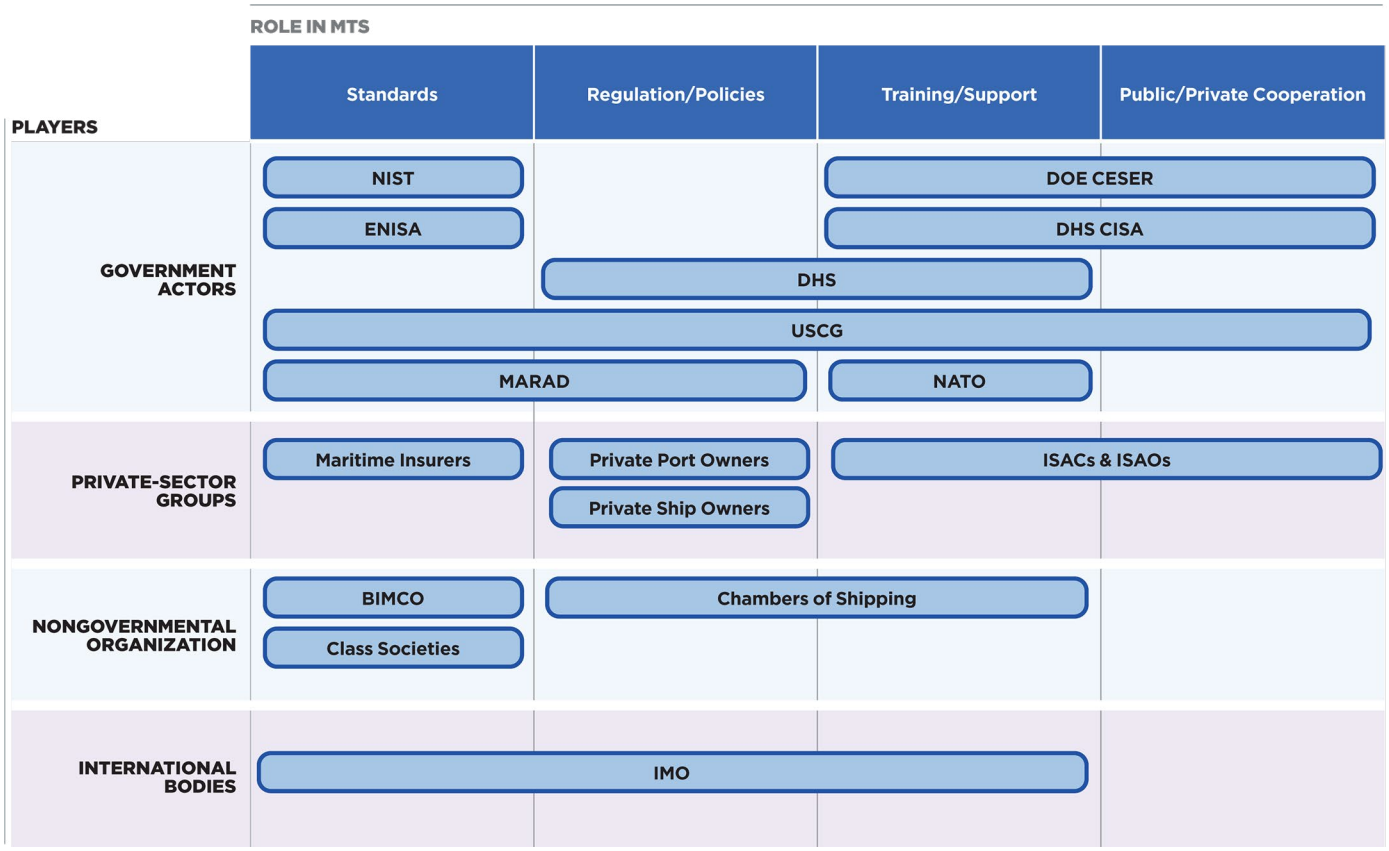
72 Cimpanu, "All Four of the World's Largest Shipping Companies."

73 Jeff Stone, "Coast Guard Says Ryuk Ransomware Hit Systems That Monitor Cargo Transfers at Maritime Facility," CyberScoop, December 30, 2019, https://www.cyberscoop.com/ryuk-coast-guard-ransomware/.

74 Cimpanu, "All Four of the World's Largest Shipping Companies."

75 Danny Palmer, "Ransomware's Perfect Target: Why One Industry Needs to Improve Cybersecurity, before It's Too Late," *ZDNet*, April 23, 2021, https://www.zdnet.com/google-amp/article/ransomwares-perfect-target-why-one-industry-needs-to-improve-cybersecurity-before-its-too-late/; and "Supply Chain Disruptions and Cyber Security in the Logistics Industry," BlueVoyant, April 22, 2021, https://resources.bluevoyant.com/hubfs/2021 Resources/BlueVoyant - Supply Chain Disruptions and Cybersecurity in Logistics - FINAL.pdf.

Key Players in the MTS



Created by Atlantic Council

and the most encompassing. Each section highlights some of the key processes and cyber risks involved—and identifies points of existing programs and relationships that can be leveraged and capitalized on to better secure the MTS.

Cybersecurity and the Life Cycle of a Ship

Ships are the heart of the maritime industry. By most historical accounts, the trading heritage of modern ocean-going vessels can be linked to the Austronesian peoples as far back as 1000 BCE.[76] Today, ships handle about 80 percent of global trade by volume and more than 61 percent of liquid energy trade.[77] They also play a key role in US national security and power projection. To address this increased demand, the evolution of ships and shipping over the ages has changed dramatically in terms of the scope of ocean-going travel, international laws and regulations, an understanding of the sea and weather, navigational methods and technologies, ship design, and so much more.

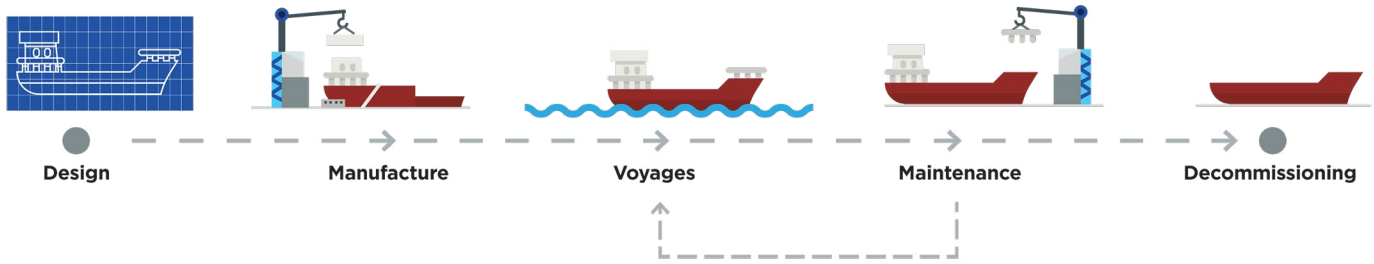
This evolution also has driven innovation in ship-based systems and their associated cyber risk due to growing technology integration and remote access by vessel shoreside management, vendors, and other essential third parties. Ships illustrate the challenge of securely designing, developing, and operating a fully connected environment—even more so when these environments look different from ship to ship. Distinct functions require specific IT and OT systems, meaning that securing each ship looks inherently different.

Protecting ships needs to be a priority. All the entities involved in the life cycle of a ship—from the designer and builder to the operator and cargo company—are susceptible to cyber threats and thus partner in this security. This section unpacks the nuances of a ship's life cycle with respect to cybersecurity by walking through how ships are designed, constructed, operated, maintained, and decommissioned. Each section highlights some of the key processes, players, and cyber risks involved, and identifies points of existing leverage that key actors can capitalize on to better secure the MTS.

76 Karan Chopra, "The History of Ships: Ancient Maritime World," *Marine Insight*, September 10, 2020, https://www.marineinsight.com/maritime-history/the-history-of-ships-ancient-maritime-world/.

77 "Review of Maritime Transport 2018," UNCTAD; and "World Oil Transit Chokepoints," EIA.

Life Cycle of a Ship



Created by Atlantic Council

Design Phase

While the primary focus of a ship's design is related to seaworthiness and operational functionality, it is only in the last one hundred years or less that ship designers have had to address nonmaritime shipboard technologies, such as those shown below:

- networks for intravessel communications and control, including everything from security, engineering, operations, and entertainment to cargo handling, ballast, intercoms, and integrated bridge systems; and note that cabling systems are directly impacted by the choice of communications devices and their protocols, affecting some aspects of ship design
- external communications networks for navigation, situational awareness, email, entertainment, radar, weather, and satellite phones, among other things
- ICS and OT equipment for vessel and cargo management, such as LNG transport

These new systems are essential for operation—yet they also must be designed and integrated securely. The computer and telecommunications networks, for example, do not merely need communication media laid out over the ship, but need to be designed and segmented in a secure fashion, necessitating cable layouts that support the secure design. Cybersecurity flaws and weaknesses introduced during the design phase and found during the shipbuilding phase will be harder and more expensive to fix.

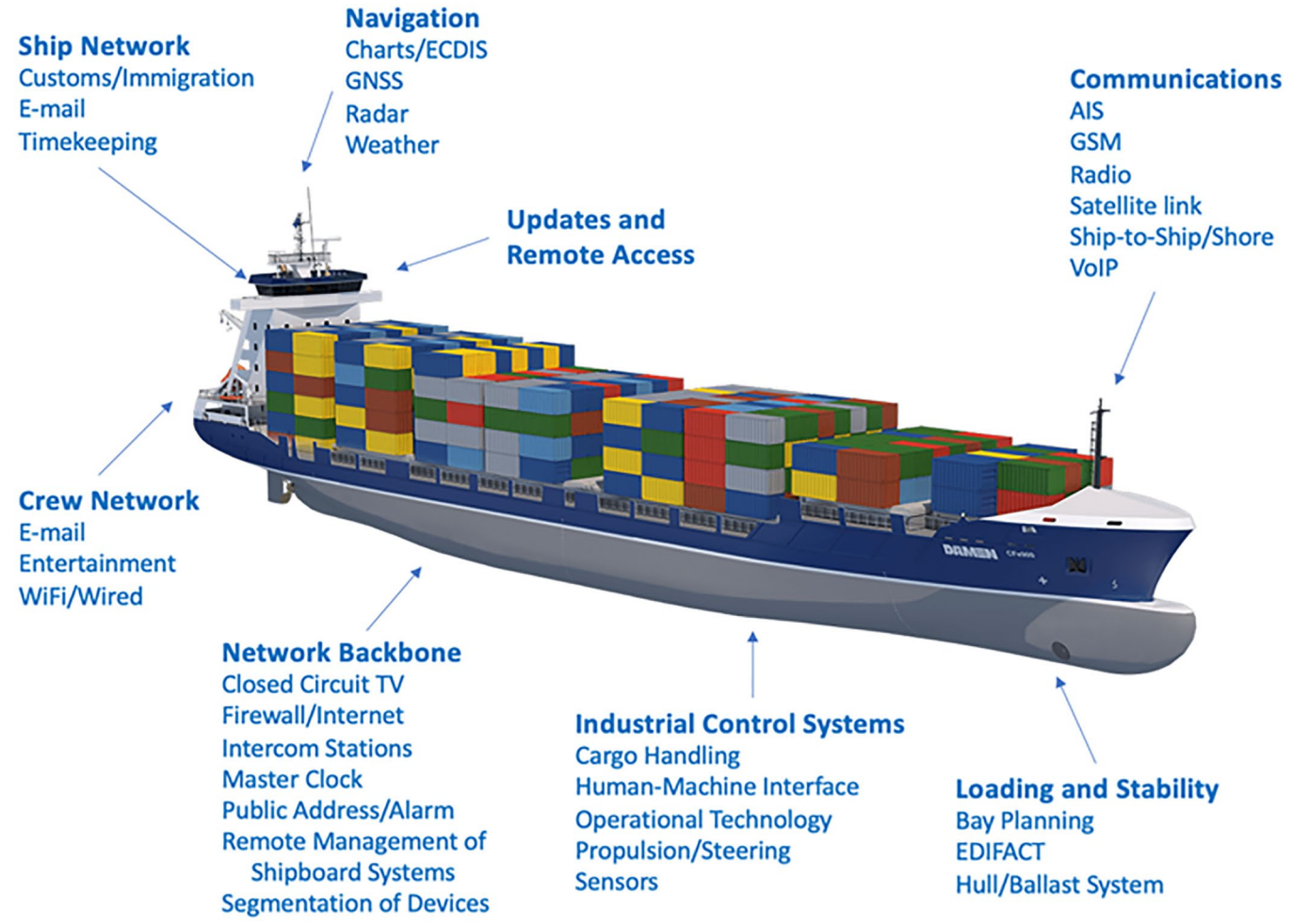
Technical standards for the design of ships are maintained by the classification, or class, societies, nongovernmental organizations that set and maintain technical standards related to the design, construction, and operation of ships and offshore structures. These standards normally focus on elements of the ship such as the ship's hull, propulsion and steering systems, power generation, and other systems related to a vessel's operation. However, these standards lag when it comes to the cybersecurity of not only these core systems but also the on-board IT and ICS systems. Securely designing every aspect of a ship and its systems is a complicated endeavor, and it looks different for every ship due to factors such as size and purpose. Certain organizations like the International Maritime Organization (IMO), the Baltic and International Maritime Council (BIMCO), and the European Union Agency for Cybersecurity (ENISA), as well as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, put forward guidelines on best practices when it comes to cybersecurity; by choosing not to be prescriptive, however, they have remained too wide-reaching to implement on a sector-to-sector basis, let alone ship to ship. Private-sector entities should work with these standards organizations to make them both easier to implement and more tailored to best practices.

The human element of cybersecurity also is a potential risk vector during the design phase. IP theft is a very real problem for designers and shipbuilders. In the past, there have been numerous incidents where foreign actors were able to get their hands on critical design IP, which has put operators in compromising positions.[78] Adversaries having intimate knowledge of ship design, connectivity, and the inner workings of critical ship systems makes defense tough, if not impossible. An adversary with access to ship design blueprints could even insert small changes, leading to flawed or even catastrophically problematic manufacturing.

In summary, although the design phase seems relatively simplistic, it is actually the starting point for cyber risk in

78 Kevin J. Hickey et al., "Intellectual Property Violations and China: Legal Remedies," Congressional Research Service, Report Prepared for the Members and Committees of the US Congress, R46532, https://fas.org/sgp/crs/row/R46532.pdf.

Shipboard Technologies



Created by Atlantic Council

ship-based maritime systems. Security in design is not just for software development—and efforts are necessary to build awareness that the ships crucial to the national economy and security must also follow the principle of whole-of-life-cycle cybersecurity.

Construction Phase

The construction of a ship at a shipyard is a tightly organized, complex choreography of the parts and people required to build a ship. As most commercial ships are built in shipyards located in South Korea, China, Japan, Italy, and elsewhere, the installation of equipment and initial cybersecurity is a commitment of trust between owners and builders. Even today, it remains an incredibly labor-intensive process with limited automation in the shipbuilding process; the construction of some of the largest vessels today can take up to two years. Managing specialized parts, block construction,[79] and the skilled labor force (e.g., electricians, carpenters, metal workers, and engineers) provides many opportunities for a cyberattack to cause huge delays and financial loss. Unauthorized modifications to the work schedule can mean that essential workers are not available when needed, causing construction delays. A cyberattacker using intelligence gleaned from the design phase could plausibly manipulate the ordering of parts to either delay the requested arrival date or to introduce the use of counterfeit or otherwise unsound components. Extraordinary care to manage the supply chain is essential to maintain the precise timing required to get a ship built on time.

79 Block construction is the method whereby different parts of the ship are built simultaneously in different parts of the shipyard, and then brought to the main vessel to be fit into place rather than constructing the vessel all in one place, one section at a time.

Ship under repair in Hamburg shipyard. Source: Pixabay

There are many ways to compromise this process. A deliberate act of sabotage or introduction of an accidental flaw during the design phase of a ship will result in a weakness in the ship's integrity. A malign actor could introduce such a flaw and alter the design plans. A small change to a blueprint can cause one block of a ship, where block construction is employed, to fit improperly with the main vessel. This becomes a more significant problem for onboard systems and software. Imagine an insider inserting a Stuxnet-type hardware vulnerability into a critical onboard system during assembly. As the global shipping industry continues its efforts to increase automation, improve efficiency, lower costs, and adjust to an increasingly digital-driven world, there is an ever-increasing reliance on software to monitor, compute, and execute critical tasks aboard a vessel—and with this reliance comes more risk.

Additionally, the 2020 Sunburst operation has shed new light on the risks associated with software and software supply-chain compromises.[80] Ships rely on software to do everything from navigate to control the internal ballast systems, which often lack adequate security configuration and thus expose them on the Internet. The Sunburst campaign has shown that operations targeting these types of systems, which in this case compromised some of the biggest players in the private and public sectors, are going to become more and more the norm for sophisticated actors with nuanced strategic aims. Preventing systems entirely from these types of compromises is a fool's errand: there simply are not enough resources in the MTS to do it. However, by better understanding the software in use and the concentration of risk on a ship, operators can better identify and mitigate potential cyberattacks as they surface. It also is important that the international maritime community, the private sector, and governments communicate extensively about these types of threats. They need to openly share attacker tactics and technical strategies for mitigation, and facilitate personnel exchanges and other forms of cross-sector and cross-national collaboration to train professionals who can understand the problems and potential

80 Trey Herr et al., *Broken Trust: Lessons from Sunburst*, Atlantic Council, March 29, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst/.

threats to the MTS from a variety of perspectives. This type of multifaceted cooperation is critical to the identification and mitigation of systemic risk in the MTS.

Operations Phase

A ship spends the bulk of its life at sea, going from port to port. As in the construction phase, a ship's operation requires a complex coordination between shipping lines, ports, departments, and agencies involved in crew acquisition and management, investors, schedulers, regulators, maritime administrators, cargo handlers, fuel and ship's stores suppliers, and more. While operating in and around US waters, ships may interact extensively with the USCG, which runs point on both law enforcement, incident response, and regulatory action for the MTS.

Supply chains are an essential linchpin to keeping a vessel on the move and operating efficiently and effectively. Ships are floating cities, complete with comparably complex computer and communications networks. A ship's internal network interconnects with the myriad systems required to keep the vessel afloat and the external network keeps it operating efficiently at sea, as seen in figure 5. There are an estimated seventy-five to eighty thousand commercial vessels on the seas today. While ships are susceptible to nearly all kinds of cyberattacks in the operations phase, one of the biggest threats are those to navigation systems, particularly jamming and spoofing the Global Navigation Satellite System (GNSS) and AIS. A small error in PNT timing can cause a large error in position (e.g., one microsecond timing error can cause a vessel to be off position by 1,000 feet, or 305 m). Issues related to PNT systems have a huge potential impact on the MTS, particularly when it comes to ship operations. Attacks on navigation system can be individually disruptive by delaying a single ship's arrival at a port or globally disruptive by causing a vessel to run aground, possibly blocking a port or waterway for days or longer. GPS spoofing has become so common in some parts of the world that many consider the system unreliable and frequently resort to navigation by other means.[81] The MTS must move rapidly and aggressively to find and employ technologies to detect, combat, and mitigate the effects of AIS and GPS spoofing. In addition, the US government and DOD need to build a resilient PNT system that is resistant to attacks on satellites.[82]

There are multiple user levels for crew accessing shipboard IT technology. Crew members access information systems for ship operations systems specific to their job function or personal use. Ships officers have significantly more widespread usage, with higher levels of access to more systems. Senior officers have access to all ship systems, particularly those assigned to shipboard and external communications functions. The ship's master, chief IT officer (if there is one), and possibly others, may have the responsibility to update computer systems, apply software patches, and maintain chart updates and other navigation systems. This approach is in line with normal cybersecurity practices around minimum necessary access; however, these varied levels of access can create their own problems. Depending on the level of access to these systems, an insider attacker with intimate knowledge of the security protocols could physically bypass access controls to access restricted areas containing critical systems. Compromises of IT systems can also come off as less significant than they actually are, which can lead to ship operators opting to not disclose an incident. It is essential to define what qualifies as a maritime cyber incident and set protocols to inform the proper public- and private-sector actors, namely the USCG and potential ports of call, that an incident has occurred. In recent years, the US Coast Guard has made essential steps to establish strong and transparent disclosure programs. However, we must also recognize that these programs are still relatively nascent - especially when compared to other sectors like financial services - and need to be further developed and matured with time and additional resources.

Additionally, crews onboard often lack a basic understanding of cyber hygiene. Yes, secure passwords have been installed on key systems, but that is undermined if the new password is placed on a sticky note next to the system access point. Social engineering attacks, phishing, ransomware, and other incident operations that directly target users are rampant across the entirety of cyberspace, and their impact on the MTS should not be underestimated. To combat this, there is real need for added training and education. There are US programs within the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) directorate, the Department of Homeland Security (DHS), and the USCG that focus on cybersecurity. However, current and future risks require more collaborative training across the public and private sectors, and more maritime-specific cybersecurity education. Although it seems like a small step, proper education on maritime cyber threats and cyber hygiene best practices can make a serious difference when it comes to mitigating risk.

Another potential vector for harm is the transport of malware from port to port, and to other ships, by an infected vessel. A 2019 simulation by the Cambridge Centre for

81 Center for Advanced Defense Studies (C4ADS), *Above Us Only Stars*, 2019, https://www.c4reports.org/aboveusonlystars; and Todd Harrison et al., *Space Threat Assessment 2020,* Center for Strategic and International Studies (CSIS), 2020, https://www.csis.org/analysis/space-threat-assessment-2020.

82 Dana A. Goward, "Assured PNT Summit–Opening Remarks," Defense Strategies Institute Assured PNT Summit, April 14, 2021, https://rntfnd.org/2021/04/16/assured-pnt-summit-opening-remarks/.

Risk Studies explored the potential impact of a computer virus carried by ships that connected to port networks.[83] In one worst-case scenario in the simulation, the malware effectively destroyed the cargo database at fifteen ports in China, Japan, Malaysia, Singapore, and South Korea, which would cause as much as $110 billion in damages—of which 92 percent ($101 billion) would be uninsured.

Securing these critical systems and processes during the operations phase is challenging. This presents one of the largest concentrations of risk in the MTS. Some of this risk is the result of lax security-development practices on the part of the private sector and inconsistent deployment of systems previously that have resulted in insecure and hard-to-defend systems. Standards bodies and regulators, such as NIST, USCG, and maritime insurers must work with the private sector to better understand and protect critical systems. However, it also is essential to work to streamline communication internationally on key mitigation strategies and vulnerability disclosures, and invest in better education for users so that they can better understand how to protect their own systems. One key facet of this is the rate at which disclosures are identified, made public, and addressed. In the past, found-yet-unmitigated vulnerabilities have remained unaddressed for as long as a full year due to poor responses to vulnerability disclosures from vendors. This cannot continue: the MTS must double down on a need for trust through a push for policies of speed, transparency, and openness around vulnerability disclosures.

Maintenance Phase

A vessel needs to move in near constant motion to produce maximum revenue. Keeping the ship operating at high capacity demands maintenance, including:

- Routine cleaning and repairs, such as repainting the hull or accommodations, or replacing worn lines and chains, and often performed while the ship is underway or at port
- Periodic refurbishment and upgrades to ship operational systems, which can include retrofitting new OT or IT systems, and requiring a short time at a maintenance yard
- A complete overhaul and rebuild, requiring an extended stay in dry dock, for hull modification, installation of new OT or IT systems, a new superstructure, or even an entire repurposing of the vessel

Even small delays in this process can yield a significant impact. The ripple effect includes the impact of how soon a ship under maintenance can get back out to sea and when the maintenance facility is available for other vessels.

The cybersecurity threats during the maintenance phase are like the construction phase, namely, financial fraud, IP theft, hacks into the work-schedule and parts-ordering systems, and supply-chain issues. However, these threats are especially prevalent in the maintenance phase because maintenance—often conducted in foreign ports—creates an opportunity for foreign-based malicious activity.

Decommissioning Phase

At the end of a vessel's life, owners decommission and, ultimately, dismantle, them. The steel used to build a vessel—that which has value—is recycled, while the rest is discarded. Ship breakers must carefully handle any hazardous materials used in construction, such as lead-based paints or asbestos, to prevent an environmental incident. Dismantling facilities are generally near water and increasingly found in developing countries, primarily in Asia.

Cybersecurity threats in this phase are similar to those of any business. Cyberfraud is of particular concern, as money changes hands for the selling and purchasing of parts and materials. Attacks on scheduling systems and databases can cause delays in the decommissioning process or mishandling of the ship's component pieces.

Key Takeaways and Points of Leverage

Ships represent a concentration of cyber risk in the MTS. They possess a complicated and differentiated risk model that can be challenging to address holistically because of the diversity of missions and systems and the opacity and lack of fundamental understanding of the threats. To push toward stronger cybersecurity postures for ships, this section identifies three points of leverage that represent key first steps for this initiative.

First, clearly ships are systemically insecure: yet a one-size-fits-all approach to security standards would not help solve what is inherently a vessel-specific problem. The global fleet is not monolithic—different ship owners and operators have different missions, different onboard systems, and thus, different risks. Transnational organizations like the IMO, in close partnership with the private sector and the class societies, must continue the existing NIST Cybersecurity Framework

83 J. Dafrron et al., *Shen Attack: Cyber Risk in Asia Pacific Ports*, Cambridge Centre for Risk Studies, 2019, pdf-cyrim-shen-attack-final-report-exec-summary.pdf (lloyds.com).

Profiles effort to provide clearer, more differentiated guidelines on cybersecurity best practices that can be implemented for specific subsections of the larger ecosystem.

Second, there is a current lack of situational awareness and collaboration in the MTS that erodes our ability to respond to emerging threats and mitigate risk on both a sector-wide and subsystem-specific basis. It is essential that the MTS expands and clarifies existing protocols and programs to streamline and incentivize information exchange and vulnerability disclosure. Whether it be through personnel exchanges, collaborative training exercises, or other forms of cross-sector and cross-national collaboration, more teamwork is essential to push forward mitigation of systemic risk in the MTS—and it must be deeper than just information exchange.

Finally, there remains a significant need for more training across the public and private sectors, as well as more maritime-specific cybersecurity education. Proper education and training on maritime cyber threats and cyber hygiene best practices can make a serious difference when it comes to mitigating risk. The United States and its key international partners must leverage preexisting training and educational programs to invest in a mandatory program for operators so that they can better understand how to protect shipboard systems and, thus, lower the systemic risk for the MTS.

As mentioned, ships are the heart of the maritime industry. Yet, the varied nature of missions and systems sets them up for failure and makes the task of widespread adaption of cybersecurity best practices a daunting one. It is impossible to increase the security of the broader MTS without addressing this.

Cybersecurity and the Life Cycle of a Port

Retired Admiral James Loy, a former USCG commandant, is widely credited with making the wry observation, "If you've seen one port, you've seen one port."[84] Ports vary widely in terms of ownership and management, the mix of civilian and military vessels and operations, the interconnection of IT systems by port operators and tenants, types and skill sets of available personnel, intermodal transportation connections, the volume and type of traffic, cargo, and passengers, types of vessels that can be accommodated, and more. That said, a port is a microcosm of all aspects of the MTS activities and processes. It is a business community, and thus it has many of the same cyber issues as any other business community.

Port operators and the USCG need to focus on securing a swath of maritime-specific systems that are critical to its effective operations. This is not an easy or cheap objective. It will take a significant investment of money and human resources from the US government to achieve.

Cyberattacks on ports share some similarities to those previously discussed relating to ships and shipping lines. Attacks often target both IT and OT systems, or the users who employ or have access to these systems. These incidents include phishing, email scams, cyberfraud, social engineering, internal threats, ineffective disposal of data devices, IP theft, and physical attacks on data storage and data systems.

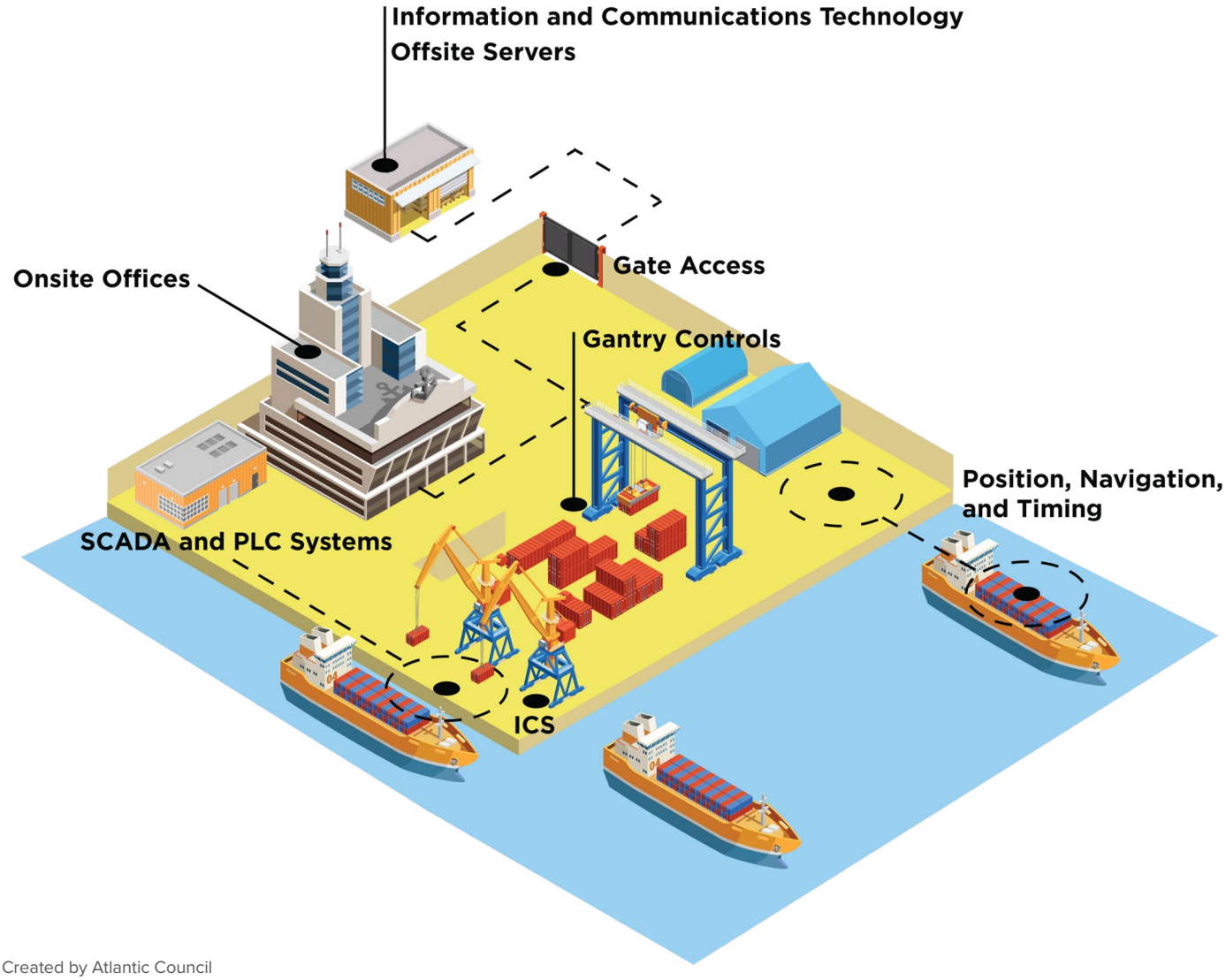
The primary role of a port is to provide an interface between sea and land transportation. On the maritime side, ports need to accommodate many types of ships, including cargo vessels (carrying liquid/dry bulk goods, oil and natural gas, containers, or general cargo), fishing boats, passenger and vehicle ships, and port service boats (such as tugs and pilot vessels). Each type of vessel has specific berthing and loading/unloading requirements and specific dock-facing systems—and thus, each will have different types of terminals and temporary storage facilities at the port. The sheer volume and variety of requisite systems at ports make cybersecurity challenging and resource intensive. A one-size-fits-all approach will leave systems wildly unprotected.

The port or government vessel traffic-management service plays a vital role in the smooth transit of vessels into, out of, and around the port area. The various maritime terminals on land handle cargo and passenger onloading and offloading, and the port's storage facilities provide at least temporary storage of cargo before a ship's arrival for loading or upon unloading. Cargo and passengers transfer to other transportation modes at the port, including automobiles, buses, trucks, railroads, inland waterway vessels, and airplanes.

Ports maintain support services for all these activities, such as berthing, cargo handling, passenger and crew accommodations, transportation within the port facility, data networking and telecommunications, and everything else needed to maintain the flow of port operations. Safety and security services are important at the port to protect personnel, passengers, and cargo, particularly in this age of ports as targets of theft, terrorism, and other hostile acts. The safety perimeter of a port is not just on land, of course, but extends out to waterways within the port's area of operation. Cybersecurity is a key element of port security—but so too is physical security.

84 Joseph Keefe, "Port Security: If You've Seen One Port, You've Seen One Port," *Maritime Logistics Professional*, March 6, 2019, https://www.maritimeprofessional.com/news/port-security-seen-port-seen-343481.

Key Elements of a Port



Created by Atlantic Council

Finally, the port must maintain services for the various agencies and other entities that have authority over some aspects of port operations. This includes the harbormaster (or the USCG's Captain of the Port), the port administrator, governmental organizations (such as the USCG, customs, immigration, and other border protection agencies), shipping companies, financial institutions, and unions. If military vessels have a presence at the port, a liaison between military and civilian authorities also will be present.

None of the functions described above occur in isolation. A lot of data moves around a port between the port authority, ships, ship operators, governmental agencies, cargo handlers, intermodal transfer companies, financial institutions, and more. As many cyberattacks have shown, when data stop moving, everything stops moving.

Unlike a ship that has distinctive life-cycle phases, a port is in continuous operation with many simultaneous data flows, where hubs of activities intersect with other segments of the MTS and beyond. From a cybersecurity perspective, consider these ICT segments within a port including the port perimeter, information and communications technology, industrial control systems, positioning, navigation, timing, and ships.

Port Perimeter

The port perimeter includes all gates for ingress and egress, the secured land-based boundary, and the line depicting the water boundary of the port's authority. The perimeter represents the first line of port security. It is at the gate and other entry points where employees, passengers, crew, contractors, vendors, and others enter and exit the port. These

employees or visitors likely enter and leave in automobiles, buses, trucks, and rail cars with passengers and cargo. Motion detectors, cameras, radiation sensors, alarms, and other access-control mechanisms monitor the movement around the gates and fences, and interconnect via networks. The port's security organization, maritime administrators, shipping agents, ship operators, immigration and customs officials, cargo handlers, logistics managers, and others must manage the movement of crew, passengers, employees, cargo, ships' stores, and goods for the port. All these activities rely on databases and other applications that are interconnected and accessible via the Internet.

After 9/11, port management and owners were entrusted to develop and maintain security, which has been described as overwhelmingly focused on physical security. However, physical security is not just reliant on guns and guards—it also is critically dependent upon network-attached cameras, sensors, alarms, and other detection equipment. These devices connect back to a central location where security personnel can check their status. Sites such as Censys and Shodan allow anyone to search for ICS devices that are accessible via the public internet.[85] Many documented reports of hacks on web-based cameras, vulnerable satellite communications systems, security devices, and IoT devices at ports (and on ships) have been recorded.[86] Vulnerabilities in these systems, if exploited, could easily hide an emerging physical security threat such as the access of an unapproved individual. As suggested earlier, supply-chain issues affect ports in two ways, with the port being part of the distribution side of the global supply chain as well as being a consumer. The necessary access—granted to a "trusted" business or trading partner—can circumvent both the cyber and physical defenses of a port. This is especially pertinent, because ports interact with so many contractors and independent businesses on a daily basis. Maintaining a proper perimeter and being able to monitor physical presence enable cyber and physical security—yet hinder it when breached.

Information Technology (IT)

The MTS is dependent upon information and ICT, and this is possibly no truer than at a port. The organization and management of all the moving parts at a port require complex algorithms to ensure the most efficient flow of people, ships, cargo, supplies, and equipment. Machine learning (ML) and artificial intelligence (AI), coupled with ICT, are increasingly critical to modern ports, particularly as they adopt smart-port technologies.

The servers hosting information at a port manage all functions found at any business, from marketing, finance and payroll, and public relations to logistics, operations, and personnel management to ship scheduling, supply-chain management, and coordination with regulators and other authorities. All systems aspects that handle personnel files, including the immigration status of passengers and crew, are here. These systems that manage port functions are a collection of servers at the port itself, third-party services, and cloud-based services. Secure telecommunications are essential for the movement of information between all these entities.

Cyberattacks against port IT infrastructures employ the same vectors as seen elsewhere in the MTS, namely, hacks into server systems, exploitation of software, and manipulation of computer users. If a bad actor cannot break the port's network defenses, a next step is to try to enter by posing as or compromising the network of another company that has legitimate access to the port's network. One particularly fruitful pathway for attacks that covers all these targets is the supply chain, where ports play two significant roles. First, shipping plays an integral role in the movement of goods in the global supply chain. Second, ports themselves receive a tremendous number of products and goods for use at the port and on ships, and thus also is a consumer at the end point of global supply chains. Both roles in the supply chain create cyberattack vulnerabilities.

Industrial Control Systems (ICS)

Port and ship use of ICS, alongside OT, is part and parcel of the creation of the smart maritime systems of the future. Faster, smaller, and cheaper computer processors, communications networks, and sensors are enabling the Maritime IoT. ICS, coupled with AI and ML, is at the heart of the emerging automation in the MTS, including operations that are remotely controlled or remotely accessed, computer assisted, and fully autonomous. OT-based automation augments port operations with smart cranes and gantries for the onloading and offloading of cargo, digital lines, and smart ports that can check and report wind speed and direction, water temperature, depth, and other information throughout the port's waters and berths. Autonomy is finding its way into docking systems, tugs, port vehicles, and drones. It is also essential for the energy sector; ICS is crucial for the transportation of oil and natural gas between refineries and ports, and ports and ships.

Attacks on ICS are particularly worrisome. CISA's Industrial Control System Joint Working Group (ICSJWG)[87] produces

85 "Home," Censys, March 26, 2021, https://censys.io/; and "The Search Engine for the Internet of Things," Shodan, https://www.shodan.io/.

86 Tucker, "Hacker Cracks Satellite Communications Network"; and Munro, "OSINT from Ship Satcoms."

87 "Industrial Control Systems Joint Working Group (ICSJWG)," Cybersecurity and Infrastructure Security Agency (CISA), https://us-cert.cisa.gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG.

Port and loading docks. Source: Pixabay

a steady stream of bulletins related to attacks on the IoT infrastructure and each new vulnerability found. One of the difficulties securing many ICS devices is the minimal user interface of the embedded devices and often limited capability to alter device settings.[88]

Maritime cyber threats in this realm include attacks on the software controlling gantries and the placement of containers, both on the vessel and in the port's staging areas. Attacks on ICS and autonomous vessels, vehicles, drones, and other systems at a port are great unknowns (e.g., autonomous docking systems and autonomous tugs), potentially altering data-gathering computers and sensors on these systems to negatively impact their operation, including causing catastrophic failures.

This is especially important for the transport of oil and natural gas. There have been several past notable cyber intrusions targeting shoreside OT energy networks including the 2017 Saudi Aramco hack,[89] and the 2018 discovery of the Triton malware.[90] With ONG networks, the stakes start higher and only go up from there. The DOE's CESER division has worked, often in partnership with the US national labs, on mitigation strategies for these types of operations. However, more can be done—and the private sector should play a significant role as it comprises the owners and operators of the majority of the systems in question.

The Cyber Security Agency of Singapore (CSA) offers a step in the right direction with its new Operational Technology Cybersecurity Expert Panel (OTCEP). With the inaugural meeting set for September 2021, the OTCEP will bring together a diverse and multinational group of experts on OT to strategize how to better protect these critical systems from attackers in the maritime domain.[91] These types of initiatives should provide a road map for international collaboration on this topic going forward.

Positioning, Navigation, and Timing (PNT)

PNT functions are essential to the successful operation of almost all aspects of modern society. GPS and other satellite-based navigation systems offer essential positioning

88 For example, start with the Hacked IoT database: "Hacked Internet of Things Database: Gadgets, Cameras, Wireless Routers," Safegadget.com, August 5, 2020, https://www.safegadget.com/139/hacked-internet-things-database/.

89 Perlroth and Krauss, "A Cyberattack in Saudi Arabia."

90 Martin Giles, "Triton Is the World's Most Murderous Malware, and It's Spreading," *MIT Technology Review*, March 5, 2019, https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/.

91 "Establishment of Operational Technology Cybersecurity Expert Panel," Cyber Security Agency of Singapore, May 3, 2021, https://www.csa.gov.sg/news/press-releases/establishment-of-operational-technology-cybersecurity-expert-panel.

information for all forms of transportation, from pedestrians and bicyclists to ships and airplanes. Timing signals from GPS satellites are essential for the proper operation of all digital network infrastructures, including mobile phone and telecommunications, television, power grids, and global banking networks. GPS is also a key component to AIS, vessel traffic-management services (VTMS), scheduling and directing vessels to a berth, surveying, dredging operations, positioning of aids to navigation, chart updates, container tracking, and more.

PNT-related issues can have a huge potential impact on ports, particularly when it comes to ship operations and port management. Attacks on the navigation system could cause a ship to crash or run aground, blocking a port or waterway for days or longer. The C4ADS report indicated that the Port of Shanghai, for example, suffered undetected GPS spoofing incidents starting in 2018 and had three hundred such events occur on one day in July 2019 alone.[92] Maritime Safety Administration (MSA) boats are frequent targets of GPS spoofing: one was spoofed 394 times in a nine-month period.[93]

AIS spoofing is another ongoing threat in port areas. Smugglers often spoof AIS signals from legitimate vessels to escape detection by the authorities. The Shanghai MSA reports that vessels carrying banned sand and gravel accounted for twenty-three collisions or allisions on the Yangtze River in 2018, with the loss of fifty-three lives.[94] In 2019, a tanker suspected of smuggling oil was sending cloned AIS signals and, reportedly, rammed an MSA patrol boat to evade capture.[95]

Clearly, bad actors will continue to exploit PNT systems in the coming years—yet the private sector has yet to produce a safer alternative. Without a more secure and defensible product, it is hard to image this problem diminishing.

Ships

While vessels in transit always fill ports, they also have fleets of local vessels, including pilot boats, tugs, local commercial fishing and cargo vessels, public safety and law enforcement boats, and recreational boats. As central hubs connecting with thousands of ships, relationships of mutual trust often exist. However, this trust is likely unwarranted and even dangerous, and the safest approach is a zero-trust model.

When it comes to cyber incidents in the MTS, the lack of a consistent threat matrix further justifies this safe approach. As an example, the Shen Attack report highlighted the potential for a visiting vessel to infect a port's network and how that infection could then spread to other ships on the network.[96] The port's network, then, becomes an amplification point in the spread of malware. To avoid this, ports must properly report and silo (or disconnect) any infected ship and its systems until resolving the compromise. However, the present lack of reporting standards leads to an erosion of the situational awareness that is essential for port law enforcement and incident responder. The MTS needs to be a step ahead of these types of threats—not a step behind. The private and public sectors need to work together to clarify incident reporting standards. Ensuring that key actors are aware of a potential breach helps address compromised systems accordingly and contain the spread.

Key Takeaways and Points of Leverage

Ships are critical to the MTS as they are the main hub for commercial interactions in the industry; yet they existentially rely on certain sets of insecure systems to facilitate these interactions. To push toward stronger cybersecurity postures for ports and their core processes, this section identifies three points of leverage that represent key first steps.

First, the sheer volume and variety of requisite systems at ports make keeping a proper cybersecurity posture a challenging and resource-intensive goal; a one-size-fits-all approach will leave many systems unprotected. As with ships, stakeholders across the international public and private sectors must work together to set guidelines and best practices for cybersecurity risk management at ports—but this is not enough. Actors seeking to improve security in the MTS must also work directly with procurement bodies, such as the Federal Acquisition Security Council (FASC), to incentivize the design of more secure systems. If systems are insecure before they ever even become part of the MTS, ports are fighting with one hand tied behind their back. Second, port security is stuck in a post 9/11 world. In 2021, the physical security of ports and the goods stored there is not just reliant on guns and guards—it is also critically dependent upon the ability of network-attached cameras, sensors, alarms, and other intrusion detection equipment to help identify human

92 Mark Harris, "Ghost Ships, Crop Circles, and Soft Gold: A GPS Mystery in Shanghai," *MIT Technology Review*, November 15, 2019, https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/.

93 Harris, "Ghost Ships, Crop Circles, and Soft Gold."

94 Harris, "Ghost Ships, Crop Circles, and Soft Gold."

95 Harris, "Ghost Ships, Crop Circles, and Soft Gold."

96 J. Daffron et al., "Shen Attack."

Unloaded cargo containers at a port. Source: Pixabay

threats. It is critical that port operators, as well as the USCG, advance an effective security mindset at ports that utilizes resources properly to secure ports from modern threats, not outdated ones. Finally, it is crucial to limit the spread of potential infections between ships and ports. The Shen report, described earlier, highlighted the potential for a visiting vessel to infect a port's network and amplify the spread of malware,[97] which represents a systemic threat to not only a port but to the global maritime ecosystem. By strictly tiering and defining what qualifies as a significant maritime cyber incident and streamlining protocols to inform the proper public- and private-sector actors in the case of an incident, the potential risk and extreme blast radius of more sophisticated incidents can be reduced.

In summary, ports are a microcosm of the larger MTS and sit firmly at the heart of the maritime industry. One single port may interact with hundreds of ships and thousands of individuals in a single day. These challenges make cybersecurity at ports a difficult and ever-evolving situation.

Cybersecurity and the Life Cycle of Cargo

The transport of cargo—whether it be tourists on a cruise ship, towering stacks of containers on a transoceanic transport ship, or oil and natural gas sealed inside the hull of a tanker ship—is the central purpose of the MTS. Outside of humans, ships today carry every imaginable type and combination of goods, in many form factors, including inland and near-coastal barges, container ships, bulk-goods cargo vessels, roll-on/roll-off (ro-ro) ships and ferries, oil tankers, and LNG carriers.

The volume of cargo transported, as well as the locations from which it ships to and from, is alone an expansive discussion. An *interactive* map, created by Kiln and University College London's Energy Institute, illuminates the diversity in missions and destinations when it comes to the global movement of cargo in the MTS.[98]

97 Shen Attack: How a Virus Could Disrupt Asia-Pacific Ports Operation," Safety4Sea, November 7, 2019, https://safety4sea.com/shen-attack-how-a-virus-could-disrupt-asia-pacific-ports-operation/.

98 Will Martin, "This Amazing Visualisation Shows How the World's Ships Move Goods around the Globe," *Business Insider*, December 23, 2017, https://www.businessinsider.com/map-of-global-shipping-interactive-2017-12; the visualization also can be seen at https://www.kiln.digital/.

Life Cycle of Cargo

Created by Atlantic Council

Matching the diversity of cargo is an ever-widening array of cyber threats facing maritime cargo transport. Many types of cyberattacks can be directed at cargo, either while it is in place or in transit. These attacks share many similarities with those on ports and ships—especially because the transportation of cargo is existentially dependent on ports and ships for transportation. Depending on the type of cargo, the types of ship- and port-based systems used for transport, and which part of the life cycle of cargo the attackers are targeting, different segments of the systemic cyber threats facing the MTS can manifest themselves as the biggest drivers of risk for cargo.

The rest of this section unpacks cargo's life cycle in the MTS by looking at cybersecurity risks posed on commercial containers and ONG products in storage, at their originating port, at sea, and when they reach their final destination. Neither intends to provide a complete picture of the type of cargo transported throughout the MTS; instead, they serve as demonstrations of where this risk can be most concentrated.

For commercial container shipping, consider the life cycle of what's called an intermodal container, due to its standard size and design so that it can travel by truck, rail, or ship. The twenty-foot equivalent unit (TEU) is the standard measure of a ship's cargo-carrying capacity, and generally corresponds to a single truck or rail car.

For the transportation of ONG products, a barrel—defined as containing 42 US gallons of liquid product—are the primary unit of measurement.[99] There are many systems that play a part in transporting ONG products, however, there are four that are most essential to the success of the transportation process: tank monitoring and storage systems; terminal transfer and pumping systems; loading racks; and automation control systems, instrumentation, valving, and metering. These systems enable critical processes throughout the cargo life cycle, and the sections below address them in detail where applicable.

Despite differing types of cargo, the routine of transporting either a commercial TEU or a barrel of ONG starts well before entering the MTS at one port and ends well after leaving the MTS:

1. Storage (Origin)
2. Port of Embarkation
3. In Transit at Sea
4. Port of Debarkation
5. Storage (Destination)

Storage

The initial storage facility, whether it be a warehouse, tank farm, or something more niche, represents the first stop for any cargo beginning its journey through the MTS. Goods in the process of shipping need safe and secure storage to protect them from potentially damaging threats such as the elements of nature, damage and destruction due to careless handling, pilferage, etc.[100] Depending on the type of cargo, these goods can often spend extended periods of time in warehouses, exposing them to a variety of threats.

Most modern storage facilities are engineering marvels that utilize large swathes of technology to facilitate key processes such as sensitive or temperature-controlled units, transport, and inventory management, among other roles. The sheer complexity of these facilities creates significant opportunity for cyberattacks during the cargo's life cycle. This can manifest in several ways. First, there has been a significant surge in automation in storage facilities. Technology intended for manufacturing now assists with distributing assets and prepping and packing them for

99 "Oil and Gas Measurement Unit," Petroleum Geology Class website, Chulalongkorn University, weebly.com.

100 Anish Wankhede, "Watch: How Container Shipping Works—The Process of Transporting Cargo in Containers," *Marine Insight*, May 27, 2020, https://www.marineinsight.com/videos/watch-how-container-shipping-works-the-process-of-transporting-cargo-in-containers/.

transport in storage facilities across the country.[101] Increased automation has also driven an increase in the need for collaborative and remote management tools. Some smart warehouses use drones or robots for moving and packing goods.[102] Warehouses also come in many shapes and sizes.[103] Public warehouses are government run and used by both public- and private-sector actors, while private warehouses are often owned by a shipper or a shipping line.

For TEUs, there are many cyber-enabled attacks on IT systems that can impact the shipper, shipping line, and warehouse prior to a container formally entering the MTS. As an example, financially motivated bad actors have proved capable of the electronic manipulation of both cargo documentation and handling systems.[104]Additionally, cyberfraud, financial fraud, false bills of lading (often used to cover up smuggling of illegal or contraband goods), cargo theft, and more can all happen by attacking the shipper's data centers and IT infrastructure, and manipulating inputs such as what is supposed to go where. IP theft also is a factor at warehouses and ports, where an intruder can learn about the contents of containers, as well as the transport schedule and other information that might have value to a competitor or adversary.[105]

OT systems in storage facilities are also vulnerable to cyber exploitation. Often, perishable products, such as food that needs to be chilled, or barrels of oil and natural gas, which must be carefully transported and stored, can be held in these warehouses. Research confirms the existence of adversary capability to disrupt the types of cooling systems used to chill a container of temperamental goods, thus causing spoilage of the contents and disrupting key shipments before they have even left their initial location.[106] Although there have been limited examples of these types of attacks on storage systems in the wild, they represent a threat vector that is a risk throughout the life cycle of cargo and a potential target for adversaries in the near future.

The human element is a huge challenge for storage as well. Like ports, storage areas can be a dynamic employment environment with employees, independent contractors, and external agents (such as truckers) moving in and out all day. Imagine an overseas manufacturer or nation-state bad actor entering a shared government warehouse to place a malicious device into containers bound for a ship with which to launch a broader cyber operation against the MTS.[107] The human element of cyber risk clearly exists for warehouses and it cannot be mitigated without a better understanding of cyber hygiene and best practices.

For ONG products, the risks associated with product storage at this point in the process looks slightly different. Storage and the security of ONG cargo while at rest is a critical concern. Yet, unlike TEUs, they are rarely placed in designated warehouses. Instead, ONG products are often stored in large oil terminals at ports, which are essentially large groupings of tanks used to store oil and natural gas before it is loaded onto vessels for transport (fig. 11).

Monitoring the status of these tanks is essential to the security and financial health of the transport process. Tank monitoring systems allow users to check fluid levels in multiple tanks, across multiple sites, from a remote location—preventing users from overfilling tanks, which is not only costly but has been known to potentially lead to fires and explosions.[108] These systems will notify users when a wide variety of problems occur, including changes in volume and fluid levels—allowing owners to assess their product, no matter where it is geographically located. However, this intersection between critical safety need and remote-monitoring capabilities makes monitoring systems a potential flashpoint for cyber risk. By shutting down or manipulating the functionality of these devices, an adversary could disguise malicious activity until it is too late to stop the potentially explosive effects.

It is true that many of the potential threats discussed here, and throughout this cargo section, have yet to be directly exploited by an adversary—at least to the authors' knowledge. However, the consequences of these potential vulnerabilities underline the fact that stakeholders in the MTS

101 Fergal Glynn, "50 Expert Warehouse Automation Tips and Best Practices," 6 River Systems, March 18, 2021, https://6river.com/warehouse-automation-tips-and-best-practices/.

102 Hari Menon, "Guide to Types of Warehouses for Shipping," *Marine Insight*, February 9, 2021, https://www.marineinsight.com/maritime-law/guide-to-types-of-warehouses-for-shipping/.

103 Menon, "Guide to Types of Warehouses."

104 Rosehana Amin, Rory Duncan, and Daniel Jones, "A Very Modern Form of Piracy: Cybercrime against the Shipping Industry—Part 1: Rapidly Developing Risks," *Lexology*, March 23, 2021, https://www.lexology.com/library/detail.aspx?g=b4dc3b52-40b5-4700-afee-a95d09b7b6d3.

105 Barry Hochfelder, "Cyber Pirates: The Latest Threat to Ocean Shipping," *Supply Chain Dive*, April 30, 2018, https://www.supplychaindive.com/news/ocean-shipping-carriers-cyber-risk/522417/.

106 Shefali Kapadia, "3 Years, 3 Cyberattacks on Major Ocean Carriers. How Can Shippers Protect Themselves?," *Supply Chain Dive*, April 29, 2020, https://www.supplychaindive.com/news/ocean-carrier-cybersecurity-maersk-msc-cosco/576754/.

107 "Cargo Theft: A Billion-Dollar Problem," *Ship Technology*, July 30, 2017, https://www.ship-technology.com/features/featurecargo-theft-a-billion-dollar-problem-5882653/.

108 Dean Mallon, "Please Enable Cookies," StackPath, February 8, 2019, https://www.piprocessinstrumentation.com/instrumentation/level-measurement/article/15564207/performing-a-storage-tank-risk-assessment.

Tank farm for crude oil storage. Source: Pixabay

need to be looking forward, not backward. A reactionary approach to addressing cybersecurity threats will not only misallocate the limited funds for cybersecurity that do exist, but also leave operators unprepared for the tactics of ever-evolving adversaries.

Originating Port

Once cargo is ready to begin its journey, it goes from the initial storage location to its port of departure via train, truck, or some other form of transportation. This process looks different for TEUs versus ONG products.

First, TEUs: after some level of inspection and verification, information about the container is entered (usually automatically) into the port's computers. The container then gets directed to a staging area, where it stays until the proper time to be moved to the designated berth and loaded onboard a ship. A container ship typically carries hundreds or thousands of TEUs. This requires a complex set of algorithms to optimize loading and unloading sequences and exact ship locations, as well as managing the ship's ballast. These algorithms need to determine a container's placement based upon the entire voyage of the vessel and knowing at which stop on the trip the container will be offloaded, special requirements for the TEU (e.g., ensuring that a container is placed in a powered bay, if required), and the load balancing needs of the ship. This complexity is the root cause of insecurity at this stage. Additionally, depending on the type of cargo, the loading process looks different; nonstandard containers and other types of goods may go through a slightly different process.

The choreography of loading (and unloading) containers is a result of messages exchanged between the shipping agents, stevedores, tonnage centers, and ship's master/cargo officer. The cybersecurity risk here can be huge. Attacks on the loading/unloading software, IP theft, cargo manifest, bayplan/stowage information, ICS/OT controllers, and more at ports can cause a misloaded vessel and harm to cargo or the ship itself, as well as other potential affects.

Attacks on ICS and OT systems can be extremely disruptive at this stage, very similar to ports, causing potential misloading or misstaging of cargo containers. A misloaded ship could be particularly vulnerable to rough seas, leading to the loss of containers overboard or other negative effects.[109] Such attacks can also damage or disable gantries, cranes, TEU containers, port vehicles, and vessels. The research firm Trend Micro demonstrated a comparable operation in 2019, proving the ability to take control of several large commercial cranes.[110] Although these types of attacks have yet to widely manifest in the MTS, they represent the next step of potential exploitations in the MTS and a clear example of the physical and economic effects of a potential attack. Port owners and operators need to work

109 Kim Link-Wills, "260 Containers Lost, 65 Damaged in Maersk Eindhoven At-sea Mishap," FreightWaves, February 19, 2021, https://www.freightwaves.com/news/260-containers-lost-65-damaged-in-maersk-eindhoven-at-sea-mishap.

110 Peter Fabris, "Hackers Can Easily Take Control of Construction Cranes," Codes and Standards content, *Building Design & Construction* magazine, January 23, 2019, https://www.bdcnetwork.com/hackers-can-easily-take-control-construction-cranes.

closely with the US government to better understand their cyber risk profile in the MTS and begin to implement best practices that can start to reduce this system risk.

This process looks distinctly different for ONG products. Before any ship planning to transport ONG can get underway, terminal transfer-line systems must move the product from the port's storage facilities to the shipside tanks. This collection of pumps and pipelines allow oil and natural gas to safely and directly travel from storage tanks at the port to storage tanks near the ships.

Once safely transferred shipside, the ONG product is loaded onto ships using loadout racks. This structure, located at a terminal or bulk plant, consists of a platform and a loading arm designed for use in loading the compartments of an oil-transport vessel. These automated systems actually load the cargo onto the ships themselves. Throughout this process, operators use metering systems to enable operators to monitor and manage the oil and natural gas that they are transporting to ensure the proper quality and volume. In some ways, consistent metering is one of the most crucial parts of this process, as product measurement is one of the clearest determinants of revenue for the industry and thus has a direct impact on profit.

To automate the process of tanking and loadout, these systems typically utilize automation platform technologies such as distributed control systems (DCS), safety instrumented systems (SIS), programmable logic controllers, process automation controllers (PAC), remote terminal units (TRU) and other remote input/output hardware (I/O).[111] Newer technology also has allowed for wireless field instrumentation and communication mesh networks that are designed for industrial area classifications in the ONG environment. Many of these systems for the last two decades have ethernet network-based communications on the processors, workstations, and network hardware and have migrated from traditionally separated systems over the years to enterprise IT networks to be even more integrated.

Owners and operators rely on these systems when moving ONG from ports to ships. However, the past has revealed flaws and operational vulnerabilities with these crucial systems—and the risks are high. First, these critical systems can be susceptible to insecure remote-access processes, leaving them potentially vulnerable for exploitation. This is a tough problem to solve, as remote access—the ability to analyze and review the performance of systems remotely, which is essential for ONG transportation—is critical in a maritime domain when it comes to safety and maintenance. However, this connectivity also inherently broadens the attack surface for these systems. Second, like the rest of the MTS, cyber risks exist during the entirety of the transport process due to a lack of knowledge of cyber hygiene in the broader operator community. One example is the use of Wi-Fi networks by crew, both onboard and at ports, which can open new avenues for exploitation and lateral movement through social engineering attacks. Finally, so-called tech bleed overrepresents another potential threat vector for these systems. Although many critical ONG systems are designed to be secure, the evolution of ship's technology over time can result in new levels of connectivity and greater exposure.

It is critical that the ICS systems that enable the secure transportation of ONG goods are better protected. Imagine the implications of a system disruption during fuel transfer between a ship and a port, resulting in an environmental spill, a significant explosion, and potential loss of life. The biggest problem when it comes to mitigating these cyber risks is that organizations do not know where to begin, and this applies to humans as well as systems. The NIST Cybersecurity Framework is a good start, but the MTS needs more specificity, especially when it comes to bulk energy operators. The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards are a good road map and should be implemented more holistically across ports that rely on these critical systems to transport ONG products.

In Transit

Once loaded up, containers and other types of cargo are then transported from the origination port to the destination port on a route that could include intermediate ports, where other containers have scheduled offloads and added cargo that needs loading.

The cybersecurity threat for cargo at sea is minimal, but not nonexistent, and it often aligns with the cyber threats discussed for ships above. A cyberattack on a cargo vessel can directly impact the cargo in transit. A refrigerated container, for example, might lose power, thus causing spoilage of the contents. Safety and monitoring devices on a bulk oil carrier might be turned off, affecting the stability of the vessel and putting lives and cargo at risk. A cyberattack on the loading/offloading systems of an LNG carrier could cause a catastrophic failure of the cooling mechanisms necessary to maintain the safe transport of the fuel. A cyberattack on the shipboard system that causes an electrical cutoff at powered bays could allow a flash-point increase near a container with flammable vapors.

A malicious actor could introduce a rogue communications device in a container to launch a cyberattack on a ship's or port's network. With some major liners exploring

111 Ryan Williams, "PLC vs. PAC vs. IPCs," *Control Engineering*, November 16, 2015, https://www.controleng.com/articles/plc-vs-pac-vs-ipcs/.

IoT-enabled containers, which customers can access remotely, the container itself may become a target vector. In most cases, ship operators do their best to ensure proper cybersecurity practices are followed, including network segmentation. However, the connectivity of these new smart containers, if accessed while onboard, could widen the attack surface for ships. This could lead to compounding effects in the operation of a ship's navigation or communications systems or, in a worst-case scenario, connect to networks at the ports to which the ship visits—leading to even more lateral movement. Although this type of operation may be rare, it only serves to further highlight the interconnected nature of the cyber threats to the MTS.

One thing to consider during this segment of cargo transportation is the ability for a cyber operation to affect physical operations. For the maritime domain, the most obvious example is pirates. A 2016 case study known as "Roman Holiday" illuminates this risk.[112] During this operation, pirates raided an anonymous shipping company multiple times. This is not irregular—pirates are known to raid commercial cargo transports. The outlier in this case, however, was that these pirates seemed to know exactly where the highest valued goods were on the ship without having to search for them. It was later identified that the company's content management system—where the ship's bills of lading lived—had been compromised. In this case, the only negative effects were stolen goods and a loss of profit. However, if you exchange the commercial goods in this scenario for, say, nuclear processing components, the potential risk of cyber-shaped physical operations becomes abundantly clear.

Destination Port

Once the cargo reaches its final destination port, the trip at sea is complete and it is time to unload. The process at the destination port is like that at the originating port, but in reverse. Oil and natural gas must pass through the same chain of systems discussed above to unload. Containers to be unloaded from a vessel need to be accurately identified, and unloading algorithms control container removal and staging. The process looks slightly different depending on the cargo, but in all cases there is a critical reliance on technology to do so.

As before, messages exchanged between shipping agents, stevedores, tonnage centers, and the ship's master/cargo officer dictate the choreography to unload the containers. Information about each container must be entered (usually automatically) into the port's computers. Customs inspections need to be managed and bills of lading need to be reviewed and inspected.

Although the attack vectors look similar for unloading ships and loading them, the potential uses for adversaries can look distinctly different. Between 2011 and 2013, a criminal group was able to gain access to the Port of Antwerp's IT systems.[113] They capitalized on this access by using it to identify and intercept the containers their international partners had filled with illicit drugs. When their access was eventually discovered and mitigated, the criminals physically broke into the facility and downloaded malware that allowed them to continue their operation unmonitored.[114] Not only does this illustrate how cyber and physical activity can intersect in the maritime domain, but it also shows how comparable risks to the cargo transportation process can manifest in diverse ways for malicious actors throughout the life cycle.

Ultimately, containers and other goods are placed onto appropriate intermodal transport to be taken off-site and transported back to a shipper or warehouse. The cybersecurity threat during this stage can be significant as well. Attacks on the loading/unloading software or ICS/OT controllers can cause a shift in the balance of a vessel or harm to cargo (or the ship). Falsified or altered bills of lading can also cover up smuggling of illegal or contraband goods, or theft of cargo.

Destination Storage

Once the cargo has been taken off the ship and processed at its destination port, it is time to make its way to its final destination. Full containers and other types of cargo eventually arrive at a distribution warehouse, where they are emptied, sorted, categorized, and the contents distributed to other forms of transport to their ultimate destination. ONG products are transferred from their ships into new tanker farms before they are eventually loaded onto other forms of transport and shipped to their final destinations.

The information security issues here are very broad and similar in almost every way to those discussed above. By attacking the shipper's critical systems, bad actors can accomplish

112 Marcus Hand, "Cyberattack Allows Pirates to Target Cargo to Steal," *Seatrade Maritime News*, July 7, 2016, https://www.seatrade-maritime.com/americas/cyber-attack-allows-pirates-target-cargo-steal.

113 "Antwerp Incident Highlights Maritime IT Security Risk," *Seatrade Maritime News*, October 21, 2013, https://www.seatrade-maritime.com/europe/antwerp-incident-highlights-maritime-it-security-risk.

114 Fred S. Roberts et al., "Combined Cyber and Physical Attacks on the Maritime Transportation System," NATO Maritime Interdiction Operational Training Centre (NMIOTC), *Maritime Interdiction Operations Journal* 18, no. 1 (2019): 27-37, https://nmiotc.nato.int/wp-content/uploads/2019/10/NMIOTC-18-2019-A-Internet.pdf.

cyberfraud, financial fraud, false bills of lading (often used to cover up the smuggling of illegal or contraband goods), IP theft, exploited OT and IT systems, cargo theft, and more. Cyberfraud and financial crimes hit shippers through fake orders or money transfers directed to the warehouse, intermodal transport companies, or the port itself. The actual theft of cargo can be directed at warehouses and ports via bogus orders, bills of lading, or shipping instructions.

Key Takeaways and Points of Leverage

Cargo is the fuel that drives the MTS and the connective tissue between ports and ships. This means that the transportation of cargo is the main profit driver for the MTS; yet the transportation of that cargo is also reliant on the ability of operators to mitigate many of the same cyber threats facing both ports and ships. To push toward stronger cybersecurity postures for the transportation of cargo, this section identifies three points of leverage that represent key first steps.

First, the transportation of cargo is an inherently interconnected business. It cannot happen without ports, ships, and shipping companies, not to mention the owner of the cargo. Shipping companies must work with ship and port owner-operators to help them facilitate the implementation of best practices and standards, and share information to protect their bottom line.

Second, industry leaders need to stop being reactive when it comes to cyber threats and start looking forward. Just as our systems continue to evolve, so will the tactics and capabilities of our adversaries. Many of the potential cyber vulnerabilities to cargo discussed in this section have not yet been exploited by malicious actors; but waiting until they are would be a critical mistake. Key stakeholders in the MTS, including the public and private sectors and academia, must follow the example of programs like GridEx, Project Evergreen, or the United Kingdom's Cyber-Ship Lab, and work to address these next-generation vulnerabilities before they are utilized by our enemies.[115]

Finally, there is a critical need to better protect the storage and transportation systems that are vital to the transportation of ONG products. These systems look different from others in the MTS and have potentially destructive consequences from as yet unexploited vulnerabilities. Implementing the NERC CIP standards for these systems would be a good first step—but it cannot be the last one.

In summary, cargo is not only the main economic driver of the MTS but also inherently relies upon ships and ports on a daily basis to make sure it can reach its final destination. This reliance leaves it vulnerable to a wider variety of threats.

115 Naveen Goud, "UK Hosts £3 Million 'Cyber Ship Lab' to Prevent Cyber Attacks on Maritime," *Cybersecurity Insiders*, November 5, 2019, https://www.cybersecurity-insiders.com/uk-hosts-3-million-cyber-ship-lab-to-prevent-cyber-attacks-on-maritime/.

4. A Collaborative Path Forward for Cybersecurity in the MTS

When plotting a course on the open ocean, conditions rarely allow a navigator to chart a straight line home. Hazards below the surface of every ocean and the unpredictability of weather systems require a crew to consistently reassess the vessel's position and adjust maneuvering to reach its destination safely. Both the captain and the crew are expected to navigate using all means available, a lens that should apply to approaching recommendations to reduce cybersecurity risks for the MTS as a whole: actors within the MTS must be capable of tapping into every available resource.

The approach to maritime cybersecurity must ultimately be holistic; even if every component of the MTS was cyber secure, the interconnection of the subsystems might not result in a secure MTS. Taking the steps necessary to build a secure maritime domain will require a better understanding of the cybersecurity-threat landscape, coupled with a segmented view of MTS infrastructure. This will allow developers, policy makers, owners, and regulators to match the best policy levers with particular maritime systems, and achieve better cybersecurity outcomes across the entire MTS.

This report puts forward twelve recommendations—split into three overarching themes—to help better secure all subsystems of the MTS from evolving cyber threats. First, stakeholders operating within the MTS must raise the baseline for cybersecurity across the maritime industry and shipping communities. Knowing is half the battle, and stakeholders must develop a sector-specific cyber risk framework, a global intelligence clearinghouse, and a common cyber-incident threat matrix, while pushing for an active, industry-wide vulnerability disclosure policy.

Second, MTS stakeholders must deepen their understanding of maritime cybersecurity and associated risks by building cross-sector linkages, especially through new professional and international exchanges between academia, industry, and government. Stakeholders must design MTS cyber-specific educational certifications to support these new workforce initiatives, with the goal of upskilling the industry and attracting talent into a cyber-aware MTS. Developers and the maritime industry must collaborate on eradicating systemic software vulnerabilities from MTS software. Lawmakers and regulators must complement these efforts by ensuring that MTS receive adequate resources to improve cybersecurity.

Third, executives and high-level stakeholders in the public and private sectors globally must prioritize cybersecurity as part of their broader risk management efforts, leveraging increased security measures and appropriate risk mitigations to help support long-term improvements in cybersecurity. MTS stakeholders should assess risk by relating their cybersecurity maturity to those of other sectors, like energy, better integrating cybersecurity with traditional maritime insurance coverage, and finally, improving cybersecurity proactively through multistakeholder simulations.

The bulk of these identified actions build on or integrate existing programs, such as the US Department of Energy-backed Cyber Testing for Resilient Industrial Control Systems (CyTRICS) program,[116] run across four national labs and the Department of Transportation (DOT) Maritime Administration (MARAD) 2021 Port Infrastructure Development Program (PIDP).[117] These programs are embedded in broader lines of policy effort and come with well-established relationships—both virtues over starting from scratch.

The maturity and effectiveness of contemporary approaches to cybersecurity in the MTS fail to reflect the vital role maritime transportation plays in supporting global commerce, diverse energy systems, and national security. Cyber threats will only continue to metastasize, accelerating both in quantity and consequence. Navigating through such turbulent waters requires an all-hands-on-deck approach—both in the United States and beyond—to improve the collective cybersecurity of the MTS.

RECOMMENDATIONS

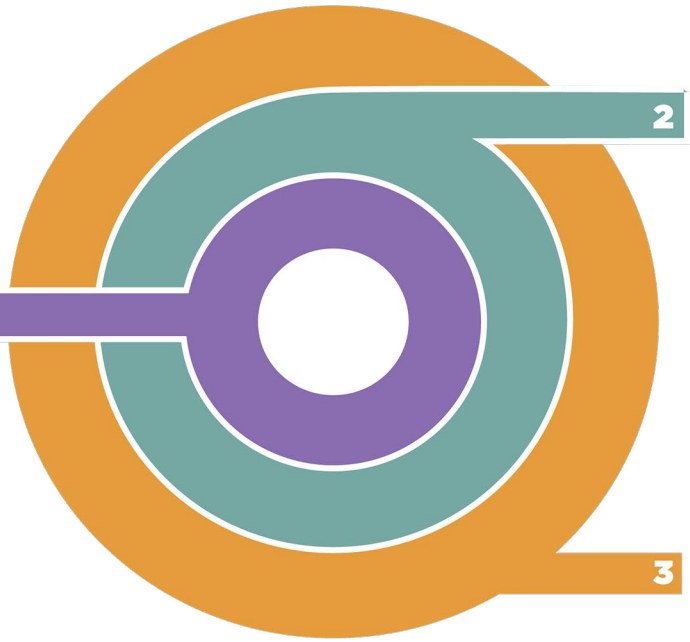
Raise the Baseline

Given the low baseline for cybersecurity in the MTS, the recommendations in this report focus on elevating the standard of cybersecurity by identifying four key problems that underpin this reality and require attention: a more specific set of cybersecurity guidelines, a clear threat matrix for maritime incidents, more streamlined intelligence sharing, and a codified vulnerability disclosure program. The

116 "Cyber Testing for Resilient Industrial Control Systems (CyTRICS)," Idaho National Laboratory, August 9, 2021, https://inl.gov/cytrics/.

117 "About Port Infrastructure Development Grants," MARAD, accessed August 16, 2021, https://www.maritime.dot.gov/PIDPgrants.

Recommendations Pinwheel



First 1

1: Drive Forward a Sector-Specific and Implementable Cybersecurity Framework

2: Define a Threat Matrix of Maritime Cyber Incidents

3: Create a Global Clearinghouse for MTS Intelligence

6: Supply Maritime Cyber Education and Certifications

7: Keep the MTS Stocked: Addressing the Resource Question

11: Plan and Simulate for Future Cyber Challenges

2 **Next**

5: Expand Cross-Sector Collaboration through Academia, Industry, and Government

8: Prioritize Better OT Security for Global Maritime Energy Networks

9: Move Past 'Guns, Gates, and Guards' Towards Cyber Risk Assessment and Management

12: Push the MTS Towards Secure Development

3 **Later**

4: Push an industry-wide transparent vulnerability disclosure policy

10: Make Cybersecurity a Core Component of Conventional Maritime Insurance

Created by Atlantic Council

recommendations in this section, numbered sequentially, seek to address these problems utilizing the points of leverage in the MTS identified in the previous life-cycle sections.

The first problem is how organizations approach security and guidelines for best practices. The IMO, the primary international maritime body, provided cybersecurity guidelines as recently as 2017, which rely heavily on the NIST Cybersecurity Framework's five functions to provide high-level direction to MTS stakeholders. Despite the IMO's guidelines, varied cybersecurity frameworks are developed and promulgated by both stakeholder organizations and multilateral bodies, such as BIMCO, the American Bureau of Shipping (ABS), and ENISA. Each framework changes and adds important elements, yet these modifications unintentionally create a tapestry of frameworks that clash at the operator level. For a sector that is already so complex in nature with a changing attack surface based on the type, function, and age of a ship or facility, cyber risk frameworks should not create added confusion.

The second problem is the need for a collective taxonomy of maritime cyber incidents and how those incidents should be logged and reported, as well as defining a minimum criterion for cybersecurity incidents to be reported. Cyber incidents will manifest differently across various sectors of the MTS. Present lack of reporting continues to erode the situational awareness that is essential for law enforcement and incident responders within the USCG to execute their mandate of prevention and response within US territorial waters and other deployment areas. The propensity for misreporting or underreporting incidents has the potential to result in the widespread compromise of critical MTS systems, which could cascade into the loss and damage of physical infrastructure, goods, and human life. The USCG should be able to accurately assess incoming ships and the ongoing cyber risk landscape of an operational area—but it will depend on an accurate incident log to do so.

The third problem is the need for more streamlined intelligence sharing within the MTS. According to the NMCP, there are more than twenty US federal organizations that have a role in the MTS. Additionally, numerous private, nongovernmental, and international organizations inundate federal organizations with an unsustainable number of intelligence requests; these varied actors are not equally able to dedicate resources to remediation efforts. The ability to quickly share intelligence with pertinent organizations is necessary but currently missing in the MTS.

The final issue is vulnerability disclosures. Vulnerabilities are inevitable; while vendors do not intentionally place

vulnerabilities within their products, their continued presence presents a credible risk to the MTS and its critical systems. However, the low prioritization of cybersecurity within the MTS has led to a lax approach to addressing vulnerabilities or known public exploits. Vulnerability disclosure must be prioritized, as the ability to quickly address known flaws is a critical step to making any ecosystem more secure.

1. Drive a Sector-Specific Cybersecurity Framework with Low Barriers to Implementation

The US government must continue and expand its role as a driver for safety guidelines within the MTS. Led by NIST, new cybersecurity framework profiles, based on the existing NIST Cybersecurity Framework, should focus on developing subsector specific guidelines and best practices for key players within the MTS that can be supported by international entities like BIMCO, ICS, and the IMO, as well as be easily adopted by industry actors.

i. Building on the existing partnership between NIST and the MITRE Corporation, NIST, in partnership with key private-sector stakeholders, should develop industry-focused cybersecurity framework profiles tailored to address the risks and needs of specific subsystems of the MTS, prioritizing key commercial and energy terminals, major shipping liners, and port systems.

ii. Led by the USCG and State Department, these profiles should be promoted to and advocated for with international partners like the EU's ENISA, as well as key international organizations such as BIMCO, ICS, and IMO. Specifically, the United States should use the inclusion of the NIST framework in IMO 2021 to push for international uniformity along a similar framework.

2. Define a Threat Matrix of Maritime Cyber Incidents

As the established incident responder within the MTS, the USCG should design a threat matrix of MTS-specific cyber incidents. This matrix should be developed in partnership with the MTS, information sharing and analysis centers (ISACs), and key insurance entities, and be accessible and usable by regulatory bodies, incident responders, and insurers to identify, assess, and log cyber vulnerability in individual vessels and facilities across the MTS.

i. Captains of US ports should establish cross-sector working groups in their individual operational regions to develop a unified threat matrix and taxonomy of incidents, and use this information to develop a new form, such as Form 2692 (Report of Marine Casualty, or OCS-related Casualty), on which operators can immediately map newly detected cybersecurity risks, vulnerabilities, and incidents to the threat matrix. Specifically, this process needs to involve key players in the insurance industry, as their frequent inspections provide them with the most extensive data and analytical capacity on risks facing the MTS.

ii. The USCG, led by the Commandant's Office and supported by DHS and the Office of the National Cyber Director, should leverage its position within the international maritime community to push this new threat matrix and taxonomy of maritime cyber incidents to the international maritime community through the IMO, specifically targeting critical trade regions and waterways, such as the Panama Canal Authority or Suez Canal Authority, that would benefit the most from such an incident matrix when it comes to systemic risk reduction.

3. Create a Global Clearinghouse for MTS Intelligence

To facilitate information sharing and prevent intelligence blockages across the global MTS, the USCG must establish a clearinghouse that can actively declassify MTS-relevant cyber-threat intelligence and provide global alerts to requisite stakeholders across the private sector and internationally.

i. With resources and operational support from the intelligence community, DHS, in collaboration with the USCG, should promote the bilateral declassification and release of MTS cyber-threat intelligence and vulnerabilities as alerts, modeled after those of DHS CISA's rumor-control online resources for 2020 election security.[118]

ii. Using its captains of the port, and in conjuction with DOT, DOE, and DHS,[119] the USCG should establish dialogue sessions focusing on clear communication channels, deconflicting roles, and streamlining collection functions across nongovernmental organizations (ISACs and ISAOs) and private companies engaged in MTS cyber-threat intelligence collection.

118 "Election Security Rumor vs. Reality," Cybersecurity and Infrastructure Security Agency website, accessed August 12, 2021, https://www.cisa.gov/rumorcontrol.

119 The captain of the port is the USCG officer who gives immediate direction to Coast Guard law enforcement activities within his or her assigned area. For more information see 33 CFR § 6.01-3 [2013], made available electronically by the Legal Information Institute, Cornell Law School, https://www.law.cornell.edu/cfr/text/33/6.01-3.

iii. Internationally, the State Department, the USCG, and DHS should separately look to engage with US allies, neighbors, and major trading partners, with the intent of creating deeper relations on information collection and sharing within the MTS. This should be explored with key maritime strategic partners such as Australia, the United Kingdom, Japan, Singapore, and the Netherlands.

4. Push an Industry-Wide, Transparent Vulnerability Disclosure Policy

The MTS, supported by the US government, should push a policy of transparency and openness around vulnerability disclosures. The business stakeholders and regulatory authorities—such as ship liners and class societies within the MTS—should work together and coordinate in encouraging software providers to follow a ninety-day disclosure policy or another mutually agreed-upon window.

i. Led by business stakeholders and regulatory bodies, this policy will affect all vendors looking to provide systems to the MTS, whether for logistics, navigation, communication, or OT processes such as the transport of oil and natural gases. To minimize potential risk, vendors should be expected to provide alternative solutions for patching when other conditions prevent normal updates.

ii. Internationally, US representatives to the IMO should propose the creation of an IMO-housed, industry-led, disclosure body that can both independently identify, and be externally notified of, vulnerabilities to MTS-specific software.

Deepen Stakeholder Awareness

The next set of recommendations focus on the need to deepen understanding of maritime cybersecurity and its associated risks, and bring attention to the requisite best practices and workforce development for mitigating these risks across the MTS. Despite the trend of increasing cyberattacks targeting the maritime community, the MTS still lags when it comes to education and training related to cybersecurity. To promote a deeper understanding of cybersecurity in the MTS, the recommendations in this section strive to address three key problems: the need for more cross-sector collaboration and knowledge exchange, the lack of maritime cyber education and training programs in the MTS, and the need for additional funding to secure the MTS.

Part of the problem in the MTS has been a lack of understanding of stakeholder perspectives, with vessel operators unaware of vendor challenges, vendors unaware of the mentality of vessel operators, and regulators often prescribing unachievable targets due to lack of visibility into the industry. For an interconnected industry like the MTS, it is challenging to holistically secure the ecosystem if stakeholders do not understand the needs and perspectives of other, differentiated actors. Existing programs such as the USCG's Marine Industry Training Program, which offers its forces "internships with maritime industry organizations and other regulatory agencies" for up to a year, are a step in the right direction. Yet, the MTS needs a more robust program, with the goal of instilling a culture of effective risk awareness, assessment, and management by encouraging exchanges between government, business, and academia to learn from one another's cybersecurity experiences.

The second key problem is the shortfall in training and education around cyber risk in the MTS. Many of the vulnerabilities in the MTS exist because of the lack of knowledge of basic cyber hygiene. Beyond the insufficient general cybersecurity knowledge across the MTS, there also is a insufficient, albeit growing, maritime cybersecurity knowledge in the incident-response community. There is a pressing need to create a cybersecurity-capable workforce, ensuring cyber literacy among the next generation of mariners and operators.

Finally, more funding within the MTS is needed to support an increased focus on cybersecurity risk mitigation—especially within the USCG given their lead role in protecting US maritime assets. As the cyber-threat landscape continues to expand and more incidents warrant governmental intervention, additional funding, personnel, and training will be required. The NMCP outlines a major push for a maritime cybersecurity workforce, which echoes the objectives outlined by the USCG's internal strategy documents to ensure that it develops a capacity to deal with MTS cyber issues. However, should the MTS threat landscape continue to grow in proportions and comparative scale, the system will quickly find itself understaffed, overburdened, and exhausted by incidents. While the multistakeholder nature of the MTS allows for greater involvement of private and nongovernmental actors in incident response, this may not be sufficient to adequately address significant cyber incidents.

5. Expand Cross-Sector Collaboration through Academia, Industry, and Government

Key US government organizations involved in the MTS—specifically, DOT, DOE, DHS, and USCG—should build upon such initiatives as USCG's Marine Industry Training Program and Idaho National Laboratory's OT Defender fellowship by bringing over key elements, including the exchange processes and the grant structure, from the United Kingdom's comparable Knowledge Transfer Partnership program. This action

can serve to not only increase the impact and scope of personnel transfers through the expansion of these programs, but also to lay out a road map for a more collaborative grant-making process that can help facilitate the scaling of these programs. Once established, these US government organizations, in partnership with the private sector, should work to expand OT Defender and the Marine Industry Training Program to include key partner states such as Australia, the United Kingdom, Japan, Singapore, and the Netherlands.

6. Supply Maritime Cyber Education and Certifications

In coordination with cybersecurity training and academic institutions, the USCG and DOT, supported by DHS and DOE, should commission curricula and industry-recognized certifications for MTS-specific OT and IT systems.

i. This task force must prioritize developing educational modules, recognized by the IMO and International Class Societies and designed in consultation with system developers, which can allow existing members of either the MTS or the cybersecurity industry to upskill and move laterally between the two industries.

ii. Led by the USCG and MARAD, this task force must share this basic MTS cybersecurity-education road map with maritime and merchant marine academies within the United States and among strategic partners, outlining a basic course structure that academies can plausibly incorporate into their existing curricula.

iii. The State Department should propose a minimum requirement of cybersecurity training for crew interacting with OT/IT and IoT systems as an amendment to the IMO's International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW).

7. Keep the MTS Stocked: Addressing the Resource Question

The White House must commit to identifying new funding for DHS that can be directed to the USCG's increased involvement in protecting and responding to cybersecurity incidents specific to the MTS.

i. Currently, the USCG earmarks approximately 10 percent, or $32.68 million, of its annual budget to cybersecurity. A 20-percent funding increase toward the USCG's activities—specifically tagged for cyber-enabling operations, cyber operations and training, maritime-sector cybersecurity engagement, and cyber protection and defenses—should be considered. This increase should be coupled with top-line relief for the USCG's whole budget, so that specific funding increases can actually be spent where they are intended to be instead of being repurposed for other projects.

ii. The USCG should use funding earmarked for maritime-sector cybersecurity engagement to expand its programs focused on working with private sector and weak state partners, to help support and facilitate a larger ecosystem shift toward more sustainable cybersecurity practices, and execute the various other activities outlined here as appropriate.

iii. Taking a page from the proposed National Cyber Reservist Force, the USCG and DHS should support the creation of a network of former cybersecurity and MTS specialists that can find employment opportunities within MTS stakeholders' firms, especially those lacking strong cybersecurity, to help raise the baseline for the ecosystem.

Collaborate on Cyber Risk

The final set of recommendations encourages MTS stakeholders to leverage every opportunity to increase awareness of the cyber risks present within the sector and prioritize, both in funding and in action, the mitigation of threats. To help push for and incentivize more prioritization of cyber risk and cyber risk mitigation the MTS, the recommendations in this section strive to address five key problems: the urgent need to better secure critical energy network OT systems; the concentrated cyber risk that is present in ports; the current role of cyber insurance in the MTS; the lack of coordinated programs focusing on forecasting future cyber threats to the MTS; and, finally, an industry-wide push toward more fundamentally secure development practices.

First, there is an urgent need to better protect ICS and OT systems for energy networks within the MTS. ONG infrastructure is highly automated, and pipeline operators, terminal owners, and utilities alike rely on ICS products for monitoring and/or remote control. As ports modernize, all manner of vessels become more digitally dependent, and as offshore energy production (e.g., oil rigs, wind turbines) turns increasingly to automated controls, the systems that undergird critical functions and processes are highly desirable and increasingly accessible targets to cyber adversaries. Critical systems throughout the MTS are vulnerable to potential exploitation, but the stakes are especially high for MTS energy networks.

Second, the MTS must do more to protect ports. Ports, in many ways, are the most important part of the MTS, as they represent the point of synthesis where most players overlap. This synthesis results in a significant concentration of cyber risk. There is precedent for ports to quickly adapt security measures to emerging threats: after 9/11, there was a serious and effective push to increase physical security that remains necessary and in place to this day. The cybersecurity threats to port operations, especially those that play critical roles in global trade and the mobilization of military forces, suggest a similar adaptation is required in the way the port industry thinks about security.

Third, there is a lack of comprehensive and well-aligned insurance coverage for owners and operators in the MTS. Cyber insurance has emerged as a major product for insurance firms; a 2019 Lloyd's report placed the potential total of premiums from cyber insurance near $25 billion by 2024.[120] Yet, simply having cyber insurance neither prevents nor protects an entity from cyberattacks.[121] In the aftermath of NotPetya, insurers informed victim organizations that they considered the attack to be an act of war, and, therefore, had negated their coverage.[122] In recent years, the broader industry has seen cyber insurance and price setting for insurance premiums emerge as a new lever to encourage adoption of better cybersecurity practices. However, cyber insurance can also have the unintended consequences of discouraging organizations from investing in cybersecurity once they consider themselves covered. The focus on physical security and safety in existing maritime insurance plans further complicates cyber insurance for the maritime sector. Reworking these policies to include more holistic cybersecurity provisions, without discouraging investment, will be a tricky line to toe. For the MTS, this adjustment is vital, as it has developed a complex web of liability and responsibility between insurers, owners, operators, crew, and ship masters.

Next, the MTS should adopt a forward-looking approach to address and respond to emerging cyber threats. The MTS has long been structured to work for a just-in-time supply model, where production and therefore supply revolves around customers' stated needs, rather than a broader and anticipatory just-in-case model that would protect the system.[123] The current mindset is not geared to cybersecurity, as the cyber threat landscape evolves on an almost daily basis. While MTS stakeholders are beginning to prioritize cyber risk in the present, they must keep a keen eye on the threats and vulnerabilities that may lie beyond the horizon.

The final key problem is the lack of knowledge and transparency around the cybersecurity of core maritime systems. As the global stakeholders within the MTS continue their efforts to increase automation, improve efficiency, lower costs, and adjust to an increasingly digital world, they will be increasingly reliant on software to monitor, compute, and execute critical tasks aboard a vessel. However, the security of these systems—and the maturity of the acquisition program that purchases these systems—does not match their criticality. System vendors exist in an ecosystem apart from the MTS and prioritize time to market, profit, and efficiency over security. As long as these attributes are deemed necessary for market competitiveness and valued over cybersecurity, the MTS will remain at a disadvantage before the fight begins.

8. Prioritize Better OT Security for Global Maritime Energy Networks

DOE CESER and FERC,[124] in close partnership with key private-sector coordination groups such as the ONG-ISAC and the Electricity ISAC (E-ISAC), should use the specter of mandatory NERC CIP standards—potentially enforceable by audits and fines for noncompliance—to drive more effective self-regulation on the security of port, shipping, and cruise systems to better the cybersecurity posture of energy and related MTS systems. Standards should be implemented in close partnership with key private-sector actors to prevent overly restrictive standards; enabling these actors to make the right decisions for the right reasons without unnecessary cost is key.

i. Starting with an ONG-ISAC led review of the most relevant policies surrounding system cybersecurity within DOE, DHS, and DOD and in consultation with the national labs, industry should work to define standards for rapidly testing and deploying patches, updates, and new hardware to mitigate cybersecurity risk in mixed IT/OT deployments for semipermanent and mobile assets, especially those operating in high-traffic areas.

120 "Lloyd's Cyber Risk Strategy," Lloyd's, 2019, https://assets.lloyds.com/assets/pdf-lloyds-cyber-strategy-2019-final/1/pdf-lloyds-cyber-strategy-2019-final.pdf.

121 Nicole Lindsey, "AIG Case Highlights Complexities of Covering Cyber-related Losses," *CPO Magazine*, October 24, 2019, https://www.cpomagazine.com/cyber-security/aig-case-highlights-complexities-of-covering-cyber-related-losses/.

122 Riley Griffin, Katherine Chiglinsky, and David Voreacos, "Was It an Act of War? That's Merck Cyber Attack's $1.3 Billion Insurance Question," *Insurance Journal*, December 3, 2019, https://www.insurancejournal.com/news/national/2019/12/03/550039.htm.

123 Harry Dempsey, "Suez Blockage Will Accelerate Global Supply Chain Shift, Says Maersk Chief," *Financial Times*, March 29, 2021, https://www.ft.com/content/e9452046-e88e-459a-9c54-341c85f3cb0d.

124 Federal Energy Regulatory Commission (website home page), accessed May 14, 2021, https://www.ferc.gov/.

ii. CESER and CISA should work with the largest actors in the private sector to mandate, or at least promote, governance-structure updates for the MTS, including the creation of a senior security and resilience position (vice president or higher) where such does not currently exist within private-sector entities. This type of position should have purview over IT and OT systems, as well as cyber and physical security, and report regularly to the chief executive officer and board of directors or equivalent.

9. Move Past "Guns, Gates, and Guards" toward Cyber Risk Assessment and Management

Through current DHS and USCG efforts led by the captains of the port function, additional funding should be identified and either allocated to FEMA's Port Security Grant Program (PSGP) and DOT MARAD's Port Infrastructure Development Program (PIDP) or earmarked to develop a dedicated port cybersecurity-improvement grant managed by MARAD. This funding should be used to expand this work, with a specific focus on dedicated grants and funding for cybersecurity assessments and developments.

i. Additionally, DHS should adapt the model deployed after 9/11 to provide more stringent requirements for cybersecurity-improvement grants, aiding the state public administrators who facilitate these federal grants. DHS should also encourage ports to take the initiative to improve their own cybersecurity, as the Port of Los Angeles has done in collaboration with IBM.[125] However, in this process, DHS and the USCG must be willing to be strict supervisors, and invite private-sector risk assessors to critically evaluate improvements, thereby ensuring improvements comply with a broader security vision for the MTS.

ii. Internationally, port operators should be encouraged by the USCG to expand their existing, and create new, international sister-port partnerships that focus on operational cybersecurity best practices. International companies should be encouraged to weigh the security advantages of collaboration on maritime cybersecurity by engaging with two sister ports.

10. Make Cybersecurity a Core Component of Conventional Maritime Insurance

Following the example of the automotive industry in recent years, insurers should push maritime clients to achieve and maintain stronger cybersecurity postures—in line with the guidelines put forward by NIST and the IMO—in exchange for premiums that reflect a commensurate level of risk reduction. Premium pricing should be benchmarked to recognize and reward those who make incremental investments toward stronger and more holistic cybersecurity practices.

i. DOT MARAD's Office of Safety should implement regulations requiring ships to possess insurance that requires mature levels of cybersecurity coverage. This can be enforced by the USCG and DHS Customs and Border Protection.

ii. Insurance companies dealing with cyber and maritime insurance should be encouraged to partner with research institutions like think tanks and the national labs to conduct long-term studies in this area to better address these emerging issues of potential financial risk.

11. Plan and Simulate for Future Cyber Challenges

The US government should utilize existing intelligence and military alliances, such as the Quadrilateral Security Dialogue (involving the United States, Japan, India, and Australia), NATO, and the Five Eyes intelligence alliance, to host international, live maritime cybersecurity-focused exercises that heavily feature private-sector involvement. While exercises already exist that focus on known vulnerabilities and perceivable threats, these efforts should be built upon and expanded to include technology vendors, ship liners, and port operators. These organizations would benefit from annual exercises forecasting risks to the MTS, and, in turn, their increased preparedness will help increase the resiliency of the broader ecosystem. There are two distinct models that should be developed.

i. Led by the USCG, key stakeholders within the global MTS should come together to participate in a series of tabletop exercises focused on identification, mitigation, and response to emerging cyber threats to the MTS. The program should be built upon the USCG's Project Evergreen Strategic Foresight Initiative and include both elements and stakeholders from the E-ISAC's annual GridEx exercise.

ii. Building upon the Army Cyber Institute's Jack Voltaic program community and NATO Locked Shields, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) should develop an

125 "IBM Works with Port of Los Angeles to Help Secure Maritime Supply Chain," Press Release, IBM (website), December 7, 2020, https://newsroom.ibm.com/2020-12-07-IBM-Works-With-Port-of-Los-Angeles-to-Help-Secure-Maritime-Supply-Chain.

international, integrated, live exercise that allows stakeholders in the MTS to practice incident response and collaboration in real time. The program should be expanded to explicitly focus on incident detection and response for ships, ports, and cargo transport operations while at sea and at rest under live conditions with allies.

12. Push the MTS toward Secure Development

Led by the International Chamber of Shipping, operators within the MTS should look to establish a solution-oriented dialogue with key global maritime manufacturers and software vendors to design a more secure software-development life-cycle maintenance process for the industry. A push by MTS stakeholders can be subsequently coupled with government efforts, led by DHS CISA, that are being considered in the wake of the Sunburst campaign. Internally, MTS businesses should be encouraged to improve their acquisition processes to require penetration testing and cyber-vulnerability assessments of technical products.

i. The MTS must work directly with entities within the US government to develop and leverage common risk-assessment processes to rigorously and proactively assess MTS system providers. Efforts must be undertaken to shift from security that is operational by intent to products that are secure by design. The MTS is continually evolving into a more connected ecosystem, yet, until that happens, vessel- and port-based products must be secure. Secure design must be the goal, and the FASC is the body best positioned to advance this effort. Internationally, the United States—led by the State Department, DOT, and key private-sector stakeholders—can work to build and petition the inclusion of these secure-by-design recommendations into a new set of cybersecurity guidelines released by the IMO to its members, like IMO 2021.

ii. In an effort led by the US Department of Commerce's (DOC) National Telecommunications and Information Administration (NTIA),[126] new products coming into the MTS should be required to provide a "software bill of materials (SBOM), a formal record containing the details and supply-chain relationships of the various components used in building software."[127] This information provides users insight into their true exposure to software supply-chain vulnerabilities and attacks, and allows operators to respond to new threats and attacks more rapidly.

iii. The DOE, in partnership with the DOE national labs and key stakeholders in industry, should push key maritime system manufacturers to buy into the DOE's Cyber Testing for Resilient Industrial Control System (CyTRICS) program to focus on accessing and protecting core OT systems for the maritime domain.[128] The program will help support cyber vulnerability testing for key systems and provide a process for sharing "findings with manufacturers to develop mitigations and alert industry stakeholders using impacted components so they can address flagged issues in their deployed systems."[129]

126 National Telecommunications and Information Administration, NTIA home page, accessed May 4, 2021, https://www.ntia.gov/.

127 Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021), https://fas.org/irp/offdocs/eo/eo-14028.pdf.

128 Office of Cybersecurity, Energy Security, and Emergency Response, "DOE CESER Partners with Schneider Electric to Strengthen Energy Sector Cybersecurity and Supply Chain Resilience," CESER News Release, US Department of Energy, September 23, 2020, https://www.energy.gov/ceser/articles/doe-ceser-partners-schneider-electric-strengthen-energy-sector-cybersecurity-and.

129 Office of Cybersecurity, "DOE CESER Partners with Schneider Electric."

5. Conclusion

The MTS is sailing into turbulent waters and needs all-hands-on-deck preparedness to guide it through cyber threats and into safe harbor. The United States has recognized the threats adversaries pose to the MTS, but it cannot address the challenge alone. A diverse set of stakeholders across the MTS must work together to mitigate maritime cyber risk.

This report works to provide an entry point for all parties within the MTS by building a cohesive picture of key life cycles within the MTS, as well as highlighting significant cybersecurity risks. Misunderstanding or underestimating the maritime cybersecurity risk landscape has real consequences for the integrity of global trade and energy markets. Everyone depends on moving resources across oceans; everyone is a stakeholder.

The MTS is changing, and with that change comes a tough set of challenges. This report's recommendations can act as an engagement plan to complement existing maritime industry and policy efforts. These efforts must open dialogue among a diverse set of industry and allied stakeholders to protect national- and economic-security interests.

Port and ship operators must move forward in the interconnected and data-rich world of the twenty-first century to better serve clients and maintain operational excellence. Yet doing so brings increased reliance on OT and IT systems that expand attack surfaces within the maritime environment, and injects new vulnerabilities for which remedies remain insufficient.

By raising the baseline for cybersecurity, deepening stakeholder awareness, and folding cybersecurity into its understanding of risk, MTS stakeholders can improve their security postures and bolster safeguards to the MTS's core role in global trade and energy.

Collaboration is key in the MTS—across the private and public sectors, within academia, and among governments the world over—to understand complex problems, better prepare for the future, and implement solutions to these pressing challenges.

Appendix 1: Players

The MTS is, at its core, a sprawling and diverse system of transportation. Each segment has its own specific purpose, set of tools, and risks. However, the MTS is a system of systems driven by the responsibilities, actions, and objectives of its players. Any ground-level understanding of the MTS must begin with a bird's-eye view of the various players in regulating, advising, informing, and driving the maritime industry, including those specifically related to maritime cybersecurity.

Baltic and International Maritime Council (BIMCO)
BIMCO is the largest international organization representing the interests of ship owners, charterers, brokers, and agents. The group's primary role is the preparation of global regulations and policy recommendations in many areas related to the MTS, from the environment, crew support, and insurance to maritime safety and security, ice information, and digitalization, including guidelines related to maritime cybersecurity. BIMCO membership comes from more than 120 countries and represents approximately 60 percent of the global merchant fleet (measured by gross tonnage of the vessels). With headquarters in Copenhagen, BIMCO has been designated a nongovernmental organization (NGO) by the United Nations.

Chambers of Shipping
National chambers of shipping (COS), such as the Chamber of Shipping of America (CSA) and the United Kingdom's Chamber of Shipping, are nongovernmental trade organizations representing the interests of a nation's shipping companies. Approximately forty national COS organizations are members of the International Chamber of Shipping, representing the interests of the maritime industry to international regulatory and standards bodies.[130] The organization strives to ensure the development, promotion, and application of best practices throughout the shipping industry, and works with key actors across the ecosystem and in the private and public sectors to do so.[131] The International Chamber of Shipping holds consultative status with the IMO.

Class Societies
Classification (or class) societies are nongovernmental organizations that set and maintain technical standards related to the design, construction, and operation of ships and offshore structures.[132] The primary focus of these standards is on a ship's hull, propulsion and steering systems, power generation, and other systems related to a vessel's operation. Class societies employ a program of inspection and certification to deliver a baseline reference point on ship safety and reliability for shipbuilders, brokers, operators, flag administrations, insurers, and the financial community. The International Association of Class Societies (IACS) has ten member organizations—including the American Bureau of Shipping (ABS), Bureau Veritas (BV, France), China Classification Society, Lloyd's Register (United Kingdom), Nippon Kaiji Kyokai (ClassNK, Japan), and the Russian Maritime Register of Shipping—and some insurers require that a vessel have a class society certification before providing coverage.[133] IACS issues advisory recommendations related to adopted resolutions: recommendation no. 166 addresses cyber resilience.[134]

Cybersecurity an Infrastructure Security Agency (CISA)
CISA is an agency within the DHS. Tasked with guiding public-sector cybersecurity strategies in the United States, CISA enhances cyber defense across all levels of government by coordinating state cybersecurity programs and improving the government's ability to repel cyberattacks (ranging from ransomware to attacks on the supply chain).[135] CISA is not an enforcement agency and has no enforcement branch; instead, it focuses on risk management and, working with public- and private-sector partners, shares threat intelligence and builds a more cyber-resilient infrastructure. CISA's Cybersecurity Division addresses many physical and cyber threats, including ICS/OT and cyber-physical system (CPS) security.

Cybersecurity, Energy Security, and Emergency Response (CESER)
CESER is an office within the DOE tasked with enhancing and improving the US energy infrastructure and supporting DOE's national security mission. By encouraging cooperation between industry, academia, DOE national laboratories, state and tribal governments, and other federal governmental agencies, CESER aims to build an energy infrastructure and supply chain that is resilient to natural

130 "About ICS," International Chamber of Shipping website, accessed May 2021, https://www.ics-shipping.org/about-ics/.

131 "About ICS," ICS.

132 "Maritime Industry Knowledge Center, Class Society," Maritime Industry Foundation website, accessed March 11, 2020, https://www.maritimeinfo.org/en/Maritime-Directory/classification-societies.

133 "IACS–International Association of Classification Societies," International Marine Consultancy (website), https://www.imcbrokers.com/iacs-international-association-of-classification-societies/.

134 IACS Recommendations 161-180, IACS website, accessed September 17, 2021, https://www.iacs.org.uk/publications/recommendations/161-180/.

135 "About CISA," Cybersecurity and Infrastructure Security Agency website, https://www.cisa.gov/about-cisa.

and human-made threats and makes the US energy sector stronger and more secure. CESER's projects include coordinating international cooperation, providing grant funding, offering training and operational support, and designing training exercises. Cybersecurity preparedness, information sharing, and incident response within the sector is emerging as a major task of the CESER office.

European Union Agency for Cybersecurity (ENISA)
Originally chartered in 2004 as the European Network and Information Security Agency, ENISA is the EU's lead agency for common standards of cyber defense throughout Europe. With headquarters in Athens, ENISA activities include the development of cybersecurity policies, cybersecurity certification programs for IT products and services, information sharing, capacity building, and cyber-awareness training programs. Recognizing the importance of the maritime sector to the EU economy and society, along with the increased digitalization of maritime facilities, ENISA has taken an active role in the preparation of maritime cybersecurity guidelines for ports.

Information Sharing and Analysis Groups
Information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs) collect, process, analyze, interpret, and share actionable intelligence related to cyber and physical threats that are relevant to their particular mission. Their overarching goal is to assist their members to maintain relevant domain situational awareness.

ISACs were defined by presidential order in the United States in 1998, during the earliest efforts to define critical infrastructures and infrastructure protection. ISACs were designed to enhance private sector/public sector information sharing to aid critical infrastructure owners and operators—the vast majority of whom are in the private sector—to protect their facilities, employees, and customers against cyber and physical security threats.

The National Council of ISACs (NCI) is composed of twenty-five member ISACs, including the Maritime ISAC, the Oil and Natural Gas ISAC (ONG-ISAC), the Electricity ISAC (E-ISAC), and Maritime Transportation Sector ISAC (MTS-ISAC).

ISAOs were formed by a 2015 US presidential order to promote voluntary information sharing within industry sectors. The goal in establishing a group of ISAOs was to enhance threat-related information sharing among organizations that did not belong to an ISAC because they were not in a clearly defined infrastructure sector. The International Association of Certified ISAOs (IACI) comprises fifteen information-sharing organizations, including the Maritime and Port ISAO (MPS-ISAO).

International Maritime Organization (IMO)
The IMO is an agency of the United Nations, headquartered in London, with a mission to develop a regulatory framework for international shipping. Its primary roles address safety, environmental concerns, legal issues, security, and international technical cooperation. It is, perhaps, best known for the Safety of Life at Sea (SOLAS) Convention, a treaty first adopted in 1914 after the sinking of the *Titanic*, and the International Convention for the Prevention of Pollution from Ships (MARPOL), first adopted in 1983. In 2017, the IMO Maritime Safety Committee released a set of Maritime Cyber Risk Management recommendations for safety-management systems that IMO encouraged shippers to implement no later than the first annual verification of a vessel's Document of Compliance and Safety Management in 2021; this resolution is known as IMO 2021.

Maritime Insurers
Maritime insurance dates back to Edward Lloyd's Coffee House in London, which opened in 1686. The coverage framework for ships and cargo is among the most mature in the insurance industry and covers damage or loss to vessels, terminals, cargo, and passengers. An increasing number of marine insurers require compliance with cyber-safety guidelines issued by class societies, the International Maritime Organization, and regulatory agencies.

National Institute of Standards and Technology (NIST)
NIST, a part of the Department of Commerce, is tasked with providing standards and guidelines for making the US technology base more secure. NIST's *Cybersecurity Framework*, created in tandem with stakeholders across the public and private sectors, focuses on putting forward a voluntary framework for reducing cyber risks to critical infrastructure based on existing standards, guidelines, and practices. The framework is considered one of the best current standards programs out there and is utilized often throughout the MTS. The framework consists of three main components: the core, implementation tiers, and profiles.

The core focuses on providing an overarching set of desired cybersecurity activities and outcomes in common terms that are easy to understand, with the goal of helping organizations reduce their cyber risk. The implementation tiers assist these organizations in implementing these activities and outcomes by providing context for what this looks like operationally. The framework profiles aim to take this a step further by identifying key requirements and objectives for specific types of organizations.

North Atlantic Treaty Organization (NATO)
NATO was born with the signing of the North Atlantic Treaty in 1949, in the aftermath of the dark days of World War II. With headquarters in Brussels, Belgium, NATO has thirty member nations in Europe and North America. As a

primarily military alliance, one of the most significant parts of the treaty is Article 5, the mutual defense clause, stating that an attack on one member country is an attack on all. This is a very controversial concept in these days of information warfare, where the very definition of *cyberwar* is not codified and an appropriate response in real space to an attack in cyberspace is not defined at all. To that end, NATO has established the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, where research, training, and exercises are conducted in the areas of technology, strategy, operations, and law. One outcome from the CCDCOE is the *Tallinn Manual*, a comprehensive guide on how existing law applies to information operations in cyberspace. This manual itself is not law, but it is the nearest guidance that is available on what constitutes a war in cyberspace.

US Department of Homeland Security (DHS)
The DHS, formed after the 9/11 attacks, is a cabinet-level agency tasked with border security, immigration and customs, disaster management and response, cybersecurity, anti-terrorism, and other efforts to protect the public within US borders. DHS also oversees the CISA and the Coast Guard.

DHS has funded a dozen Science and Technology (S&T) Centers of Excellence (COE) addressing a range of multidisciplinary technology solutions for homeland security. Of particular interest to maritime cybersecurity is the Maritime Security Center (MSC) at Stevens Institute of Technology.

US Coast Guard (USCG)
The US Coast Guard is an agency within the DHS, although it can be transferred to the DOD to operate as part of the US Navy in times of war or when ordered by the president. The Coast Guard has a unique role in the US military, as it has a law-enforcement function in both US and international waters, and has a federal regulatory function. USCG functions also include search and rescue, security throughout the MTS, drug interdiction, port-facility inspection, public boating safety, maintenance of aids to navigation, and fishery regulation enforcement.

Broadly speaking, the Coast Guard's role related to cybersecurity is twofold. First, it must keep the security of USCG ICT assets, including systems and networks used to manage and maintain USCG operations and shipboard systems. Second, the Coast Guard assists in the cyber protection of information assets throughout the MTS, including at port facilities and on civilian vessels via the creation of Cyber Protection Teams (CPTs). Coast Guard Cyber Command (CGCYBER) is a part of the DOD's US Cyber Command (USCYBERCOM), primarily for external facing threats and attacks, while its internal mission is the preparation of its cyber workforce.

US Maritime Administration (MARAD)
MARAD is an agency of the Department of Transportation, responsible for administering funds to develop, promote, and work the US maritime fleet. MARAD maintains the National Defense Reserve Fleet (NDRF), a collection of vessels that can be put into service in a national emergency. MARAD also operates the US Merchant Marine Academy, one of the five US service academies.

Key International Actors/Programs
There are a number of international activities related to maritime cybersecurity that are examples of some of the initiatives that will undoubtedly become more common and widespread in the future. This is by no means an exhaustive list but one that is representative of the response to the need to prioritize cybersecurity in the MTS.

- In 2018, the International Maritime Cyber Centre of Excellence (IMCCE) opened in Singapore. Created by an industry group headed by Wärtsilä and Templar Executives, the center is composed of a Maritime Cyber Emergency Response Team (MCERT) to provide cyber intelligence, incident support, and real-time cyberattack assistance, and a Cyber Security Reporting Portal (CSRP). The center also offers cybersecurity training. In 2019, the Maritime and Port Authority of Singapore (MPA) opened the Maritime Cybersecurity Operations Centre to conduct nonstop monitoring and correlation of cyber events across all maritime critical infrastructures. This center also offers early incident detection, monitoring, analysis, and response, and provides a link to the Singapore Port Operations Control Centre to more quickly respond to events.

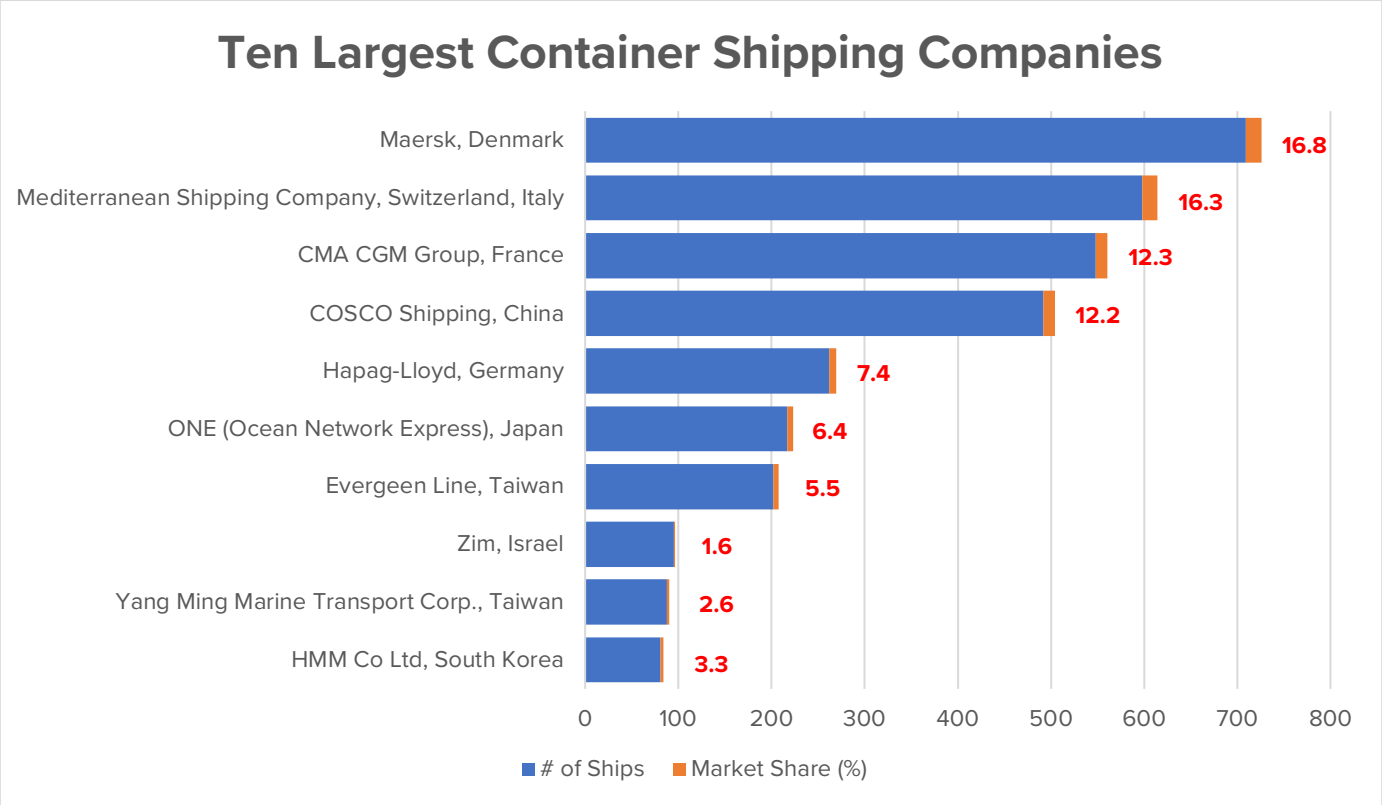
- The Tallinn University of Technology is located just blocks away from NATO's CCDCOE. In 2020, the Centre for Digital Forensics and Cyber Security and the Estonian Maritime Academy, both part of TalTech, received a grant from the EU to establish a Maritime Cyber Security Centre to help develop cybersecurity in the maritime domain.

- An industry-academic partnership in Canada is forming a maritime cybersecurity research and development center. Announced in early 2021, cybersecurity professors at Polytechnique Montréal are teaming with maritime companies Davie Canada and Neptune Cyber to build Canada's Maritime Cyber Security Centre of Excellence. The goal of the five-year research program is to examine cybersecurity in maritime critical infrastructures and build better systems to detect and respond to malicious cyber activity.

Key Private-Sector Actors

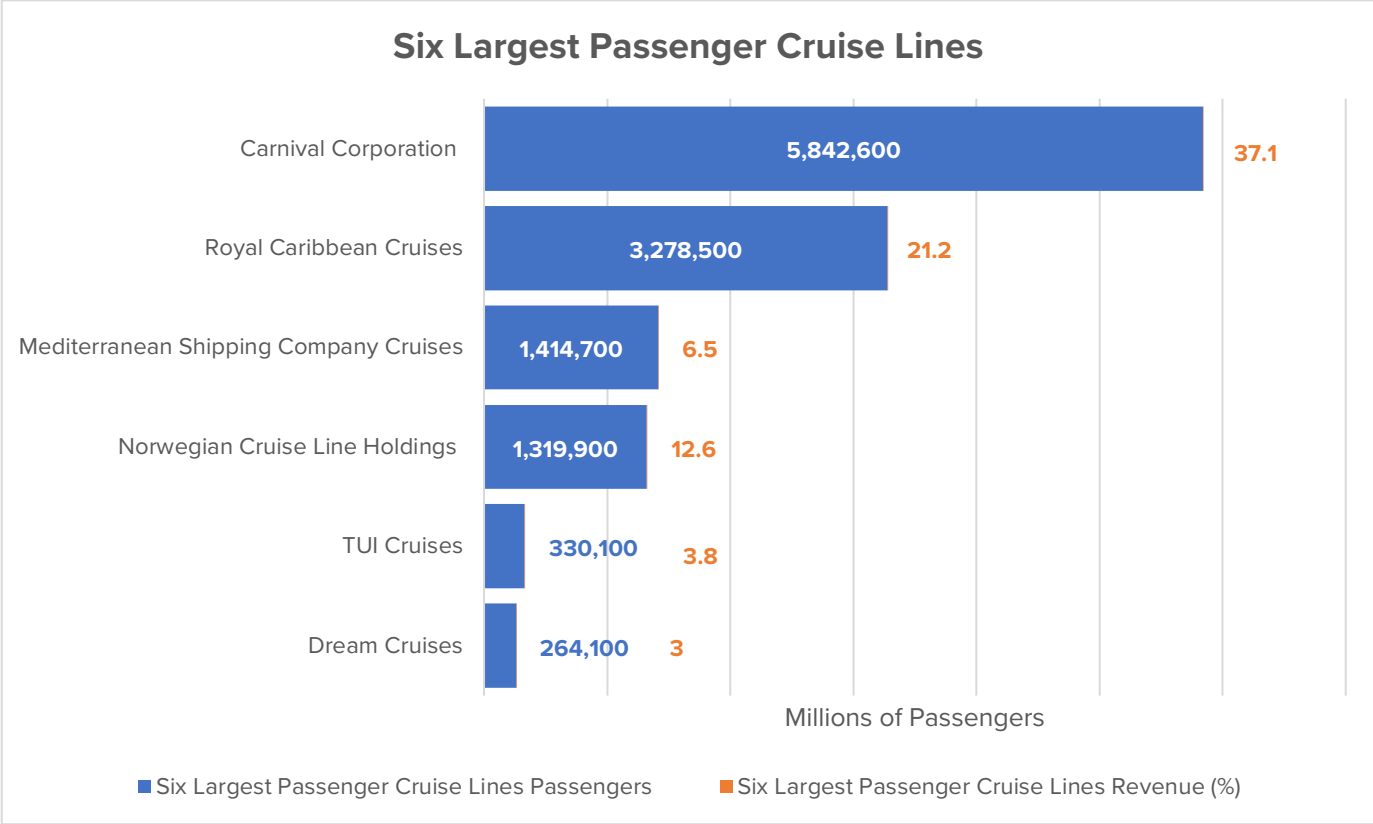
The MTS is a critical element of global and national economic security. It is the anchoring industry for the bulk of imports and exports. Responsible for the transport of food, goods, and people, the MTS partners in many sectors for the public good. The vast majority of MTS assets are owned and/or operated by the private sector.

The global merchant fleet is composed of more than fifty-six thousand cargo vessels, including general and bulk cargo carriers, various types of tankers, and vehicle/passenger vessels.[136] The table below lists the ten largest container shipping companies, comprising 84 percent of the global market.



136 "Global Merchant Fleet: Number of Ships by Type," Statista, March 4, 2021, https://www.statista.com/statistics/264024/number-of-merchant-ships-worldwide-by-type/.

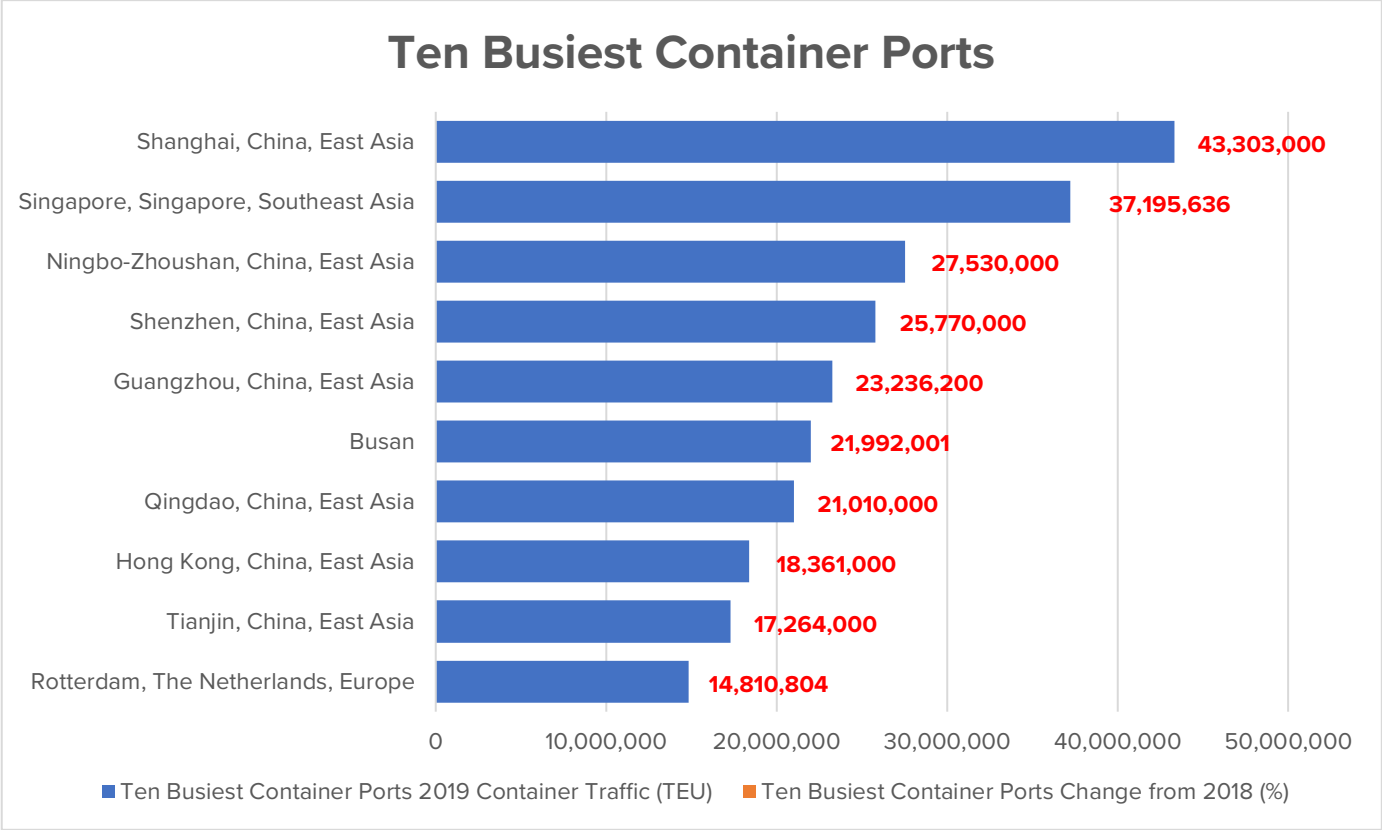
The table below lists the largest oceanic passenger cruise lines, comprising nearly 95 percent of the global market share. Cruise lines represent a significant segment of the larger maritime business community, even if they are not explicitly addressed at length in this report.

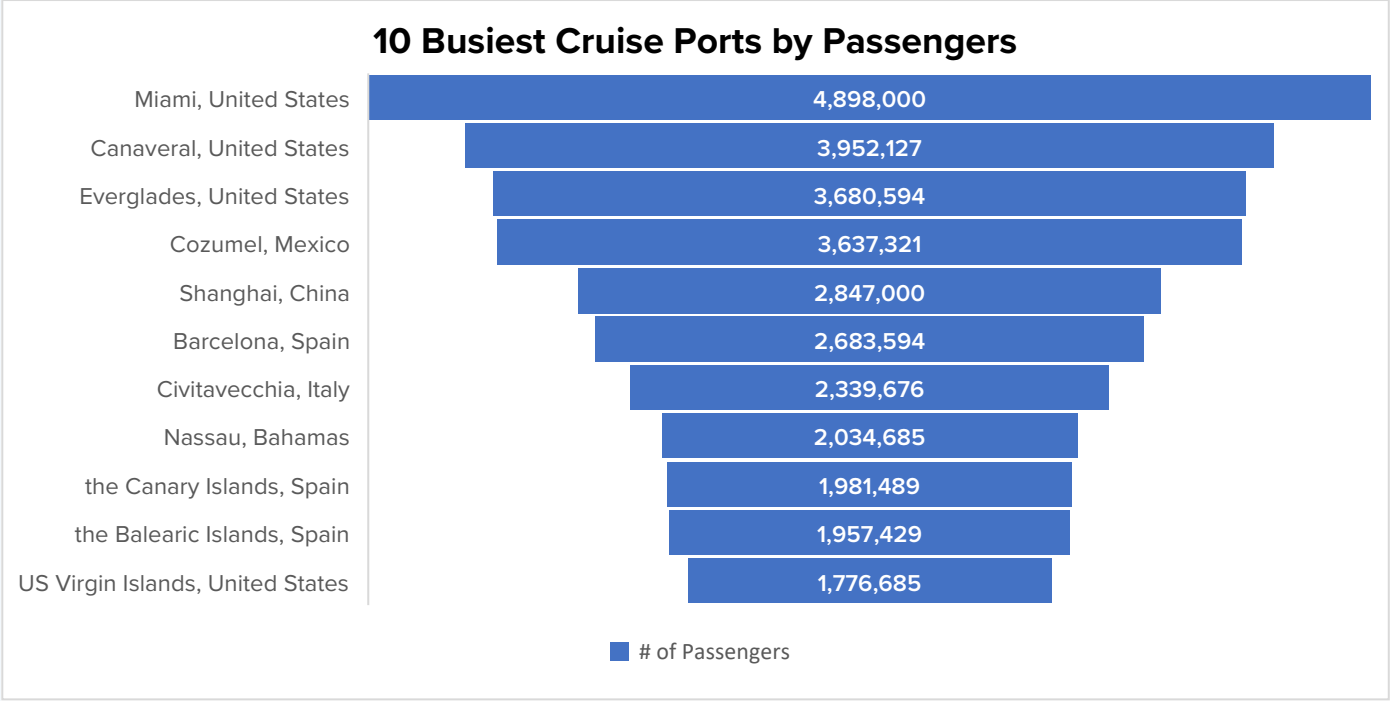


As of 2019, 93 percent of global shipbuilding took place in China, Japan, and the Republic of Korea, and Asian countries owned half of the world's fleet. A large number of commercial vessels are registered under a flag that matches neither the country of the builder nor the owner or operator; the top five flag registrants are Panama, Liberia, Marshall Islands, Hong Kong, and Singapore, with Panama alone accounting for 16 percent of the global commercial fleet.[137]

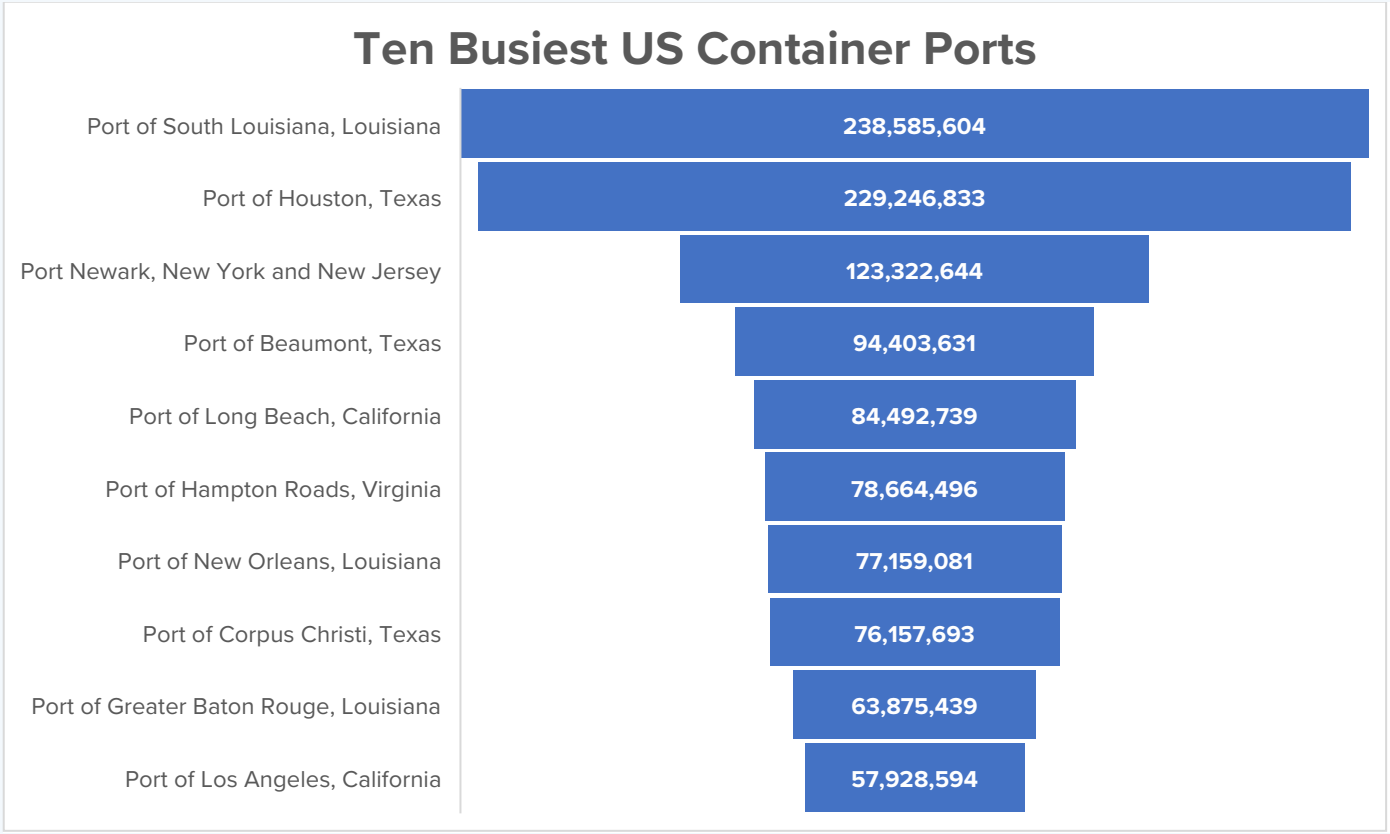
While ships and shipping companies have been, in general, private-sector entities (albeit some with a close relationship to the respective national government), the same cannot be said of ports around the world. Ports vary in ownership and operation, covering the spectrum from being fully operated by a public-sector governmental agency to being owned and/or operated by a private-sector—possibly foreign—company. The two tables below show the location of the busiest ports in the world. Not surprisingly, the top ten busiest container ports are all in Asia, all but one in the east or southeast portion of that region. Also, not surprisingly, six of the top ten busiest passenger ports—including the top five—are in the Caribbean.

137 "2020 E-handbook of Statistics: Merchant Fleet," UNCTAD, December 7, 2020, https://stats.unctad.org/handbook/MaritimeTransport/MerchantFleet.html.





The United States is a maritime nation and, like others in the global economy and supply chain, dependent upon shipping for trade. The table below lists the ten busiest US container ports, where the busiest, the Port of Los Angeles, is the seventeenth busiest in the world. Nearly half the US import/export volume goes through three ports. The critical nature of these ports to the US economy and security becomes immediately evident, given the number of ships and cargo that move through two adjoining ports on the West Coast and two on the East Coast. All these ten ports are owned, and most are operated, by some sort of municipal or other governmental agency; like a private-sector business, all are tasked with making a profit.


Ten Busiest US Container Ports
Port of South Louisiana, Louisiana
238,585,604
Port of Houston, Texas
229,246,833
Port Newark, New York and New Jersey
123,322,644
Port of Beaumont, Texas
94,403,631
Port of Long Beach, California
84,492,739
Port of Hampton Roads, Virginia
78,664,496
Port of New Orleans, Louisiana
77,159,081
Port of Corpus Christi, Texas
76,157,693
Port of Greater Baton Rouge, Louisiana
63,875,439
Port of Los Angeles, California
57,928,594

Appendix 2: Acronyms

- 2020 National Maritime Cybersecurity Plan (2020 NMCP)
- 2021 Port Infrastructure Development Program (PIDP)
- A. P. Moller-Maersk Group (Maersk)
- Application programming interface (API)
- Artificial intelligence (AI)
- Automatic identification system (AIS)
- Baltic and International Maritime Council (BIMCO)
- Center for Advanced Defense Studies (C4ADS)
- Chamber of Shipping of America (CSA)
- Chambers of Shipping (COS)
- China Ocean Shipping Company (COSCO)
- Coast Guard Cyber Command (CGCYBER)
- Cooperative Cyber Defence Centre of Excellence (CCDCOE)
- Customer relationship management (CRM)
- Cyber protection teams (CPTs)
- Cyber Security Agency of Singapore (CSA)
- Cybersecurity and Infrastructure Security Agency (CISA)
- Distributed control systems (DCS)
- Enterprise resource planning (ERP)
- European Union Agency for Cybersecurity (ENISA)
- Federal Acquisition Security Council (FASC)
- Federal Emergency Management Agency (FEMA)
- Five Eyes (FVEY)
- Global Positioning System (GPS)
- Gross domestic product (GDP)
- Industrial control system (ICS)
- Industrial Control System Joint Working Group (ICSJWG)
- Information communications technology (ICT)
- Information sharing and analysis centers (ISACs)
- Information sharing and analysis organizations (ISAOs)
- Information technology (IT)
- Input/output hardware (I/O)
- Intellectual property (IP)
- International Association of Class Societies (IACS)
- International Convention for the Prevention of Pollution from Ships (MARPOL)
- International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW)
- International Maritime Organization (IMO)
- International Ship and Port Facility Security Code (ISPS)
- Internet of Things (IoT)
- Machine learning (ML)
- Marine Safety Information Bulletin
- Maritime Safety Administration (MSA)
- Maritime Security Council (MSC)
- Maritime transportation System (MTS)
- Mediterranean Shipping Company (MSC)
- National Cyber Security Centre of the Netherlands (NCSC)
- National Institute of Standards and Technology (NIST)
- National Maritime Cybersecurity Plan (NMCP)
- National Telecommunications and Information Administration (NTIA)
- National Transportation Safety Board (NTSB)
- Nongovernmental organizations (NGOs)
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
- Oil and natural gas (ONG)
- Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC)
- Operating systems (OS)
- Operational technology (OT)
- Operational Technology Cybersecurity Expert Panel (OTCEP)
- Personally identifiable information (PII)
- Port Security Grant Program (PSGP)
- Positioning, navigation, and timing (PNT)
- Process automation controllers (PAC)

- Programmable logic controllers (PLC)
- Protected health information (PHI)
- Remote terminal units (TRU)
- Safety instrumented systems (SIS)
- Safety of Life at Sea Convention (SOLAS)
- Social Security number (SSN)
- Software Bill of Materials (SBOM)
- Supervisory control and data acquisition (SCADA)
- Tactics, techniques, and procedures (TTP)
- Twenty-foot equivalent unit (TEU)
- US Coast Guard (USCG)
- US Department of Commerce (DOC)
- US Department of Defense (DOD)
- US Department of Energy (DOE)
- US Department of Transportation (DOT)
- Vessel traffic management services (VTMS)

Acknowledgments & Author Bios

This project would not have been possible without the support of Idaho National Laboratory and the Department of Energy. Specifically, the authors would like to thank Virginia Wright, Geri Elizondo, Andrew Bochman, Tim Conway, Frederick Ferrer, Rob Pate, Sean Plankey, Nick Anderson, and Puesh Kumar.

Thank you to the staff and researchers who supported this project from its inception, including Trey Herr, Madison Lockett, and Emma Schroeder. Thank you to Nancy Messieh and Andrea Ratiu for their support in managing the digital design and web interactivity of this report, and to Donald Partyka for designing the report's graphics. For their peer review, the authors thank Alex Soukhanov, Suzanne Lemieux, and Marco Ayala.

Thank you to the participants of the various workshops held over the past year for feedback on this effort and to the numerous individuals who lent their insights and expertise with the authors during that time.

AUTHOR BIOGRAPHIES

William Loomis is an assistant director with the Atlantic Council's Cyber Statecraft Initiative within the Scowcroft Center for Strategy and Security. In this role, he manages a wide range of projects at the nexus of geopolitics and national security with cyberspace, with a focus on software supply chain security and maritime cybersecurity. Prior to joining the Atlantic Council, he worked on market research and strategy at an emerging technology start-up in Madrid, Spain. He is also a certified Bourbon Steward.

Virpratap Vikram Singh is a consultant with the Atlantic Council's Cyber Statecraft Initiative within the Scowcroft Center for Strategy and Security. He is the Cyber and Digital Fellow for the Saving Cyberspace Project at Columbia University's School of International and Public Affairs, supporting research and programming pertaining to cyber conflict and cybersecurity policy. Over the last two years, he has designed and authored multiple scenarios for the Initiative's Cyber 9/12 Strategy Challenges in New York, Austin, and Washington D.C. Previously, he worked as the Digital Media and Content Manager for Gateway House, a foreign policy think tank in Mumbai. He holds a Master in International Affairs (International Security Policy) from Columbia University's School of International and Public Affairs and a BA in Liberal Arts (Media Studies and International Relations) from the Symbiosis School for Liberal Arts.

Gary C. Kessler, PhD, CISSP, is a nonresident senior fellow with the Atlantic Council's Cyber Statecraft Initiative. He is president of Gary Kessler Associates, a consulting, research, and training company located in Ormond Beach, Florida, and a principal consultant at Fathom5, a maritime digital services company headquartered in Austin, TX. He has been in the informationsecurity field for more than 40 years. Gary is the co-auhor of "Maritime Cybersecurity: A Guide for Leaders and Managers," as well as more than 75 other papers, articles, books,andb ook chapters about information security, digital forensics, and technology. He has been a speaker at national and international conferences for nearly 30 years.

Xavier Bellekens is a nonresident senior fellow with the Atlantic Council's Cyber Statecraft Initiative within the Scowcroft Center for Strategy and Security. He is the CEO of Lupovis Defence, and used to work as an Assistant Professor and Chancellor's Fellow in the Institute for Signals, Sensors and Communications with the Department of Electronic and Electrical Engineering at the University of Strathclyde, Scotland. His experience spans from cyber-defence, deception, deterrence and attribution of cyber-threats in critical infrastructures to cyber-situational awareness and cyber psychology and cyber-diplomacy.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor, Washington, DC 20005

(202) 463-7226, *www.AtlanticCouncil.org*