U.S. Maritime Trade and Port Cybersecurity

Vulnerabilities within the Maritime Transportation System Caused by Foreign Adversarial Access to Port Equipment and Supply Chain Management Systems

Team Members:
Daniel B, U.S. Coast Guard and Government Team Lead
Ben Trowbridge, Outsourcing Center LLC and Private Sector Team Lead
Scott B, DHS I&A
Marisa B, Texas Department of Public Safety
Christopher Curran, Thomson Reuters Special Services
Justin Freeh, Ncyber
Lee Kim, Keytera Corporation
Nicholas K, TRANSCOM
Lauren Moore, National Cyber-Forensics & Training Alliance
Chan Hong Park, American Express
Sara T, U.S. Coast Guard

Team Champions:
Amy S, Federal Maritime Commission
Robert L, DHS Office of Policy

2023
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

COVER IMAGE: PORT OF TACOMA, STATE OF WASHINGTON

DISCLAIMER STATEMENT: The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Companies whose analysts participated in the Public- Private Analytic Exchange Program. This document is provided for educational and informational purposes only and may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and the product of joint public and private sector efforts.

ABSTRACT

The U.S. Maritime Trade and Port Cybersecurity team examined the current threat landscape, challenges, and mitigations affecting the maritime trade and port sector. In an increasingly connected world, the security of our ports is paramount. The interconnected network of third-party vendors, and the foreign acquisitions of U.S. port infrastructure, present significant vulnerabilities for U.S. port authorities. While significant advances have occurred in recent years, more improvement is needed to ensure this sector is adequately protected from current and future threats. Vulnerabilities, whether old or new, must be addressed before cyber adversaries are able to compromise critical systems and assets within ports.

In this report, the team examines the challenges to U.S. port facilities from foreign investment and application programming interfaces. Worldwide maritime ports, facilities, and infrastructure are vulnerable to physical and cybersecurity exposure through foreign adversarial access to port equipment and supply chain information management systems. Specifically, proprietary foreign adversarial companies manufacture, install, and maintain port equipment that poses potential vulnerabilities to global maritime infrastructure information technology and operational technology systems. Utilizing a case study related to the issue of foreign cranes in U.S. ports, the team highlights challenges, vulnerabilities, and recommended courses of action regarding how to mitigate potential vulnerabilities introduced by foreign investment in U.S. ports.

Similarly, port community systems enable the exchange of information between private and public organizations operating within the port environment, increasing efficiency, and promoting ease of business while simultaneously introducing vulnerabilities to the system. Unauthorized access to port community systems would likely enable adversaries to collect large sets of data on the U.S. supply chain and the ability to delay/disrupt the maritime transportation system (MTS). Port community systems offer unique services tailored to best support the operations conducted at a port facility. Common services include terminal control, container status reporting, and scheduling/booking requests and confirmations. Utilizing a case study related to the issue of the vulnerabilities introduced through improperly configured scheduling systems and interfaces, the team highlights challenges, vulnerabilities, and recommended courses of action on how port facilities can better secure access points to their networks.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

Interview Participants

The research team wishes to express its gratitude to the DHS Public-Private Analytic Exchange Program for the opportunity to explore the current threat landscape, challenges, and mitigations affecting the maritime trade and port sector. The topic is timely for our increasingly connected world, making the security of U.S. ports paramount. We would also like to thank the University of Houston and the Port of the Future Conference for hosting our team and allowing us to present our preliminary findings and engage in dynamic discussions with conference attendees, who provided excellent feedback and thoughts on the direction of this project. Further, we would like to thank the Northwest Seaport Alliance, Tacoma Rail, Husky Terminal, and the Tacoma Crane Maintenance Team for hosting our team and providing knowledge and insights that helped inform the direction of this report. We also thank the members of the Cybersecurity and Infrastructure Security Agency (CISA) Region 10 and U.S. Coast Guard (USCG) Sector Puget Sound staff for their perspectives on the risks presented to the MTS. Additionally, we acknowledge exemplary support from the American Association of Port Authorities (AAPA) for allowing AEP team members to participate in a facilitated panel discussion at the Smart Ports Seminar & Expo 2023. Finally, we would like to thank the following subject matter experts who provided their time and insights on vulnerabilities within the MTS: Michael E, Audrey E, Alfred G, Robert H, Joshua M, Stephen M, Sean P, Jeremy R, and Ken W.

AEP Team Members

Member	Title and Organization
Daniel B, Government Team Lead	Operations Support Department Head, U.S. Coast Guard Cyber Command
Ben Trowbridge, Private Sector Team Lead	Cyber and Technology Strategic Advisor, Outsourcing Center LLC
Scott B	Regional Intelligence Analyst, DHS I&A
Marisa B	Maritime Intelligence Analyst, Texas DPS
Christopher Curran	Analyst, Thomson Reuters Special Services
Justin Freeh	President, Ncyber
Lee Kim	President, Keytera Corporation
Nicholas K	Intelligence Analyst, TRANSCOM
Lauren Moore	Intelligence Team Lead, National Cyber-Forensics & Training Alliance
Chan Hong Park	Information Security Specialist, American Express
Sara T	Junior Officer Cryptologic Career Program Intern, U.S. Coast Guard
Champion: Amy S	**Director of Maritime Supply Chain Analytics, Federal Maritime Commission**
Champion: Robert L	**Policy Analyst, DHS CIRR**

EXECUTIVE SUMMARY

U.S. ports are essential components of the global supply chain, facilitating the movement of goods and passengers across domestic and international borders. The continued growth of port and network systems is critical for a robust U.S. economic and strategic system. As technology and automation become increasingly integrated into port operations, interconnectivity is emerging as a key driver of efficiency and economic growth. However, the growing interconnectivity of ports increases the attack surface and the number of vulnerabilities within port networks leverageable by malicious cyber actors. To maintain economic security, the U.S. must adopt a comprehensive risk management approach and secure network ports based on cooperation and close partnership between government and industry.

This paper explores the risks of using foreign-owned and developed technology, and tangentially foreign investment, in U.S. ports. Further consideration is given to specific technologies, such as application program interfaces (APIs) that can provide attackers increased access to a facility's network, examining a possible use case scenario. The case presented also highlights the potential impacts on both public and private sector equities, and the paper provides actionable recommendations to mitigate some of the risks presented. It also highlights future challenges to the MTS, such as artificial intelligence and the incorporation of ship management systems into a port's network operations. The paper concludes with an assessment of the future of maritime trade and port cybersecurity, noting the current obstacles to achieving the goal of securing U.S. maritime trade.

KEY FINDINGS

Based on our research and analysis we identified the following key findings:

- Physical-cyber infrastructure, such as port operational equipment, may provide attackers opportunities to conduct cyberattacks that physically disrupt port operations if vulnerabilities are found.
- Application program interfaces (APIs), if not designed with security in mind, can facilitate access and lateral movement through a port and third-party vendor networks to implement cyberattacks.
- Supply chain risk management (SCRM) based approach can help ports stay secure as they increasingly outsource services to remain competitive.
- Communication and trust between government entities and port facilities are vital for the rapid identification, containment, mitigation, and recovery of cyberattacks on port facilities.

OVERVIEW OF THE MARITIME TRANSPORTATION SYSTEM (MTS)

U.S. ports are essential components of the global supply chain, facilitating the movement of goods and passengers across domestic and international borders. The continued proliferation of port and network systems is critical for a strong U.S. economic and strategic system. As technology and automation have become increasingly integrated into port operations, interconnectivity is emerging as a key driver of efficiency and economic growth. However, the increased interconnectivity of ports also creates a larger attack surface by introducing more vulnerabilities to port networks leverageable by malicious cyber actors. To maintain economic security, the U.S. must adopt a comprehensive risk management approach and secure network ports.

> "**Regardless of the level of digital adoption...a port or port facility may be [at], the unavoidable handmaiden to digitalization is cyber risk. No port or port facility is immune to it.** Given that the majority of cyber-attacks involve people and fragmented system landscapes, every port and port facility is at risk. Moreover, the inequalities of the digital divide and the burdensome role the maritime industry plays at the center of global trade and information exchange underscores the shared nature of cyber risk within the global port and port facility community."—IAPH Cybersecurity Guidelines for Ports and Port Facilities, International Association of Ports and Harbors (IAPH), Version 1.0, 2021[1]

This paper defines port interconnectivity as the integration, information, and communication technology in port operations—including information technology (IT), operational technology (OT), and industrial control systems (ICS)/supervisory control and data acquisition (SCADA) systems, port community systems, and automated identification systems (AIS)—to facilitate real-time data sharing and coordination among port stakeholders. The increase in port interconnectivity and the resulting vulnerabilities have been a growing concern among security professionals in the maritime trade and port cybersecurity domain.

Given the necessity of interactions between dozens to hundreds of entities, port facilities potentially have hundreds to thousands of network access points and application programming interfaces (APIs) that could allow hostile actors to gain a foothold and maintain persistent access to the network. To increase efficiency and productivity, ports connect, communicate, and share data with a variety of third-party stakeholders, including intermodal landside connection operators (i.e., freight rail, pipelines, and trucking) and other critical infrastructure sector facilities operating at the port (i.e., assets under the Energy or Chemical Sectors) (see Figure 1). While interconnectivity offers significant operational benefits, it also introduces potentially exploitable vulnerabilities that increases the cyberattack surface. Cybersecurity threats, disruptions to communication networks, and vulnerabilities in automated control systems are some of the key risks to be mitigated.

[1] [1] (U) | International Association of Ports and Harbors | Pub 2021-07-02 | IAPH Cybersecurity Guidelines for Ports and Port Facilities, Version 1.0 | Technical Report | https://safety4sea.com/wp-content/uploads/2021/09/IAPH-Cybersecurity-Guidelines-2021_09.pdf

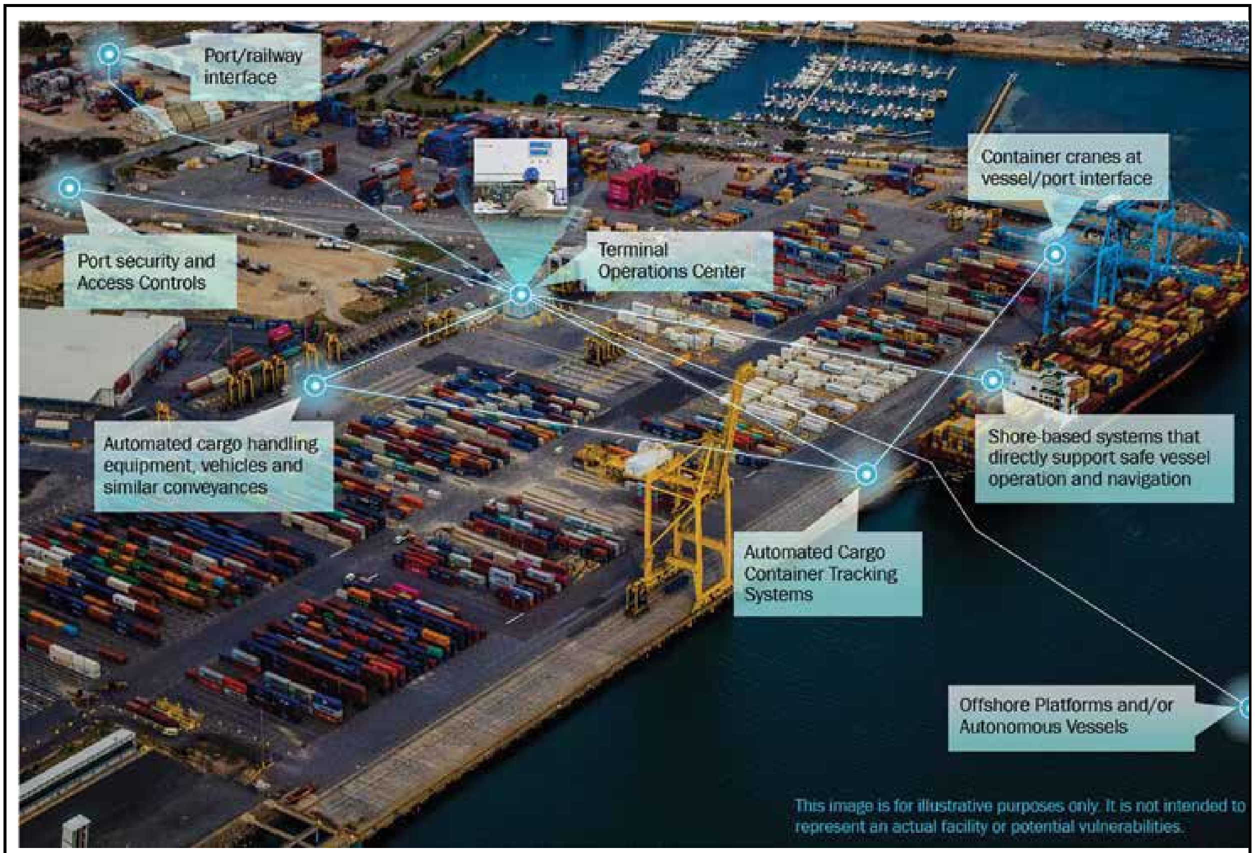

Port/railway interface
Port security and Access Controls
Terminal Operations Center
Container cranes at vessel/port interface
Automated cargo handling equipment, vehicles and similar conveyances
Shore-based systems that directly support safe vessel operation and navigation
Automated Cargo Container Tracking Systems
Offshore Platforms and/or Autonomous Vessels
This image is for illustrative purposes only. It is not intended to represent an actual facility or potential vulnerabilities.

Figure 1. Interconnected infrastructure at ports for cyber security considerations.[2]

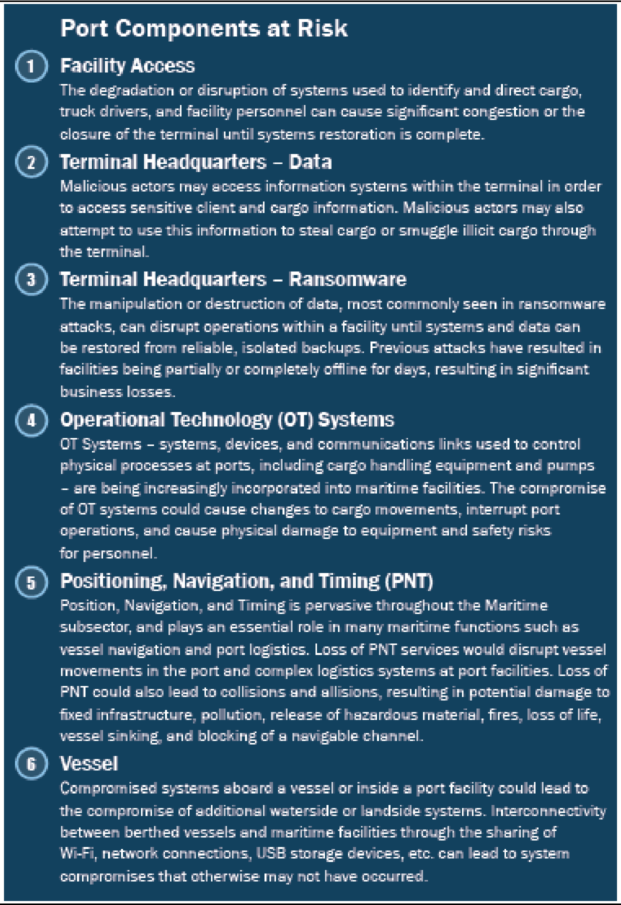
Due to the interconnectivity of the U.S. maritime transportation system, cyber incidents targeting one facility or terminal operator may negatively impact local port operations and potentially create supply chain disruptions, compromise cargo and passenger safety, and disrupt critical infrastructure operations.

One example of how cybersecurity vulnerabilities can impact maritime port operations is the 2017 NotPetya wiper malware attack. This attack targeted a Ukrainian software company, but it quickly spread to other countries and industries, including maritime shipping companies with U.S. operations. Once the malware successfully infected one computer, the malware spread across the company's network and disrupted operations at several major ports, including the Port of Rotterdam and the Port of Los Angeles, causing significant delays in cargo shipments, and creating a ripple effect across the global supply chain.[3]

[2] (U) | U.S. Coast Guard | Pub August 2021 | Cyber Strategic Outlook | https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf
[3] (U) | Bloomberg | Pub 2023-06-14 | Pro-Russian Hackers Target Website of Europe's Largest Port | Online News Article | https://www.bloomberg.com/news/articles/2023-06-14/pro-russian-hackers-target-website-of-europe-s-largest-port-in-rotterdam#xj4y7vzkg

> **"It turns out one single infection was responsible for the Maersk compromise. M.E.Doc had been installed on a company computer in Odessa, a Ukrainian port city on the Black Sea.** This was all NotPetya needed to infect the entire system. Across the globe, port facilities shut down, and tens of thousands of truckloads of goods were turned away. Maersk's entire booking system went down, as well as the complex loading systems used to systematically load container ships to avoid capsizing them. Maersk was dead in the water."—Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk, Industrial Cybersecurity Pulse 2021[4]

In a 2020 infographic report, seen as Figure 2, the Cybersecurity and Infrastructure Security Agency (CISA) noted cyberattacks targeting OT systems could have serious consequences for maritime port operations, including potential physical harm to personnel, equipment, and cargo.[5]



Port Components at Risk

1 **Facility Access**
The degradation or disruption of systems used to identify and direct cargo, truck drivers, and facility personnel can cause significant congestion or the closure of the terminal until systems restoration is complete.

2 **Terminal Headquarters – Data**
Malicious actors may access information systems within the terminal in order to access sensitive client and cargo information. Malicious actors may also attempt to use this information to steal cargo or smuggle illicit cargo through the terminal.

3 **Terminal Headquarters – Ransomware**
The manipulation or destruction of data, most commonly seen in ransomware attacks, can disrupt operations within a facility until systems and data can be restored from reliable, isolated backups. Previous attacks have resulted in facilities being partially or completely offline for days, resulting in significant business losses.

4 **Operational Technology (OT) Systems**
OT Systems – systems, devices, and communications links used to control physical processes at ports, including cargo handling equipment and pumps – are being increasingly incorporated into maritime facilities. The compromise of OT systems could cause changes to cargo movements, interrupt port operations, and cause physical damage to equipment and safety risks for personnel.

5 **Positioning, Navigation, and Timing (PNT)**
Position, Navigation, and Timing is pervasive throughout the Maritime subsector, and plays an essential role in many maritime functions such as vessel navigation and port logistics. Loss of PNT services would disrupt vessel movements in the port and complex logistics systems at port facilities. Loss of PNT could also lead to collisions and allisions, resulting in potential damage to fixed infrastructure, pollution, release of hazardous material, fires, loss of life, vessel sinking, and blocking of a navigable channel.

6 **Vessel**
Compromised systems aboard a vessel or inside a port facility could lead to the compromise of additional waterside or landside systems. Interconnectivity between berthed vessels and maritime facilities through the sharing of Wi-Fi, network connections, USB storage devices, etc. can lead to system compromises that otherwise may not have occurred.

[4] (U) | Industrial Cybersecurity Pulse | Pub 2021-09-30 | Throwback Attack: How NotPetya accidently took down global shipping giant Maersk | Online News Article | https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/

[5] (TLP:WHITE) | CISA | December 2020 | Port Facility Cybersecurity Risks | Infographic | https://www.cisa.gov/sites/default/files/publications/port-facility-cybersecurity-risks-infographic_508.pdf

Figure 2. CISA Infographic regarding port cybersecurity vulnerabilities.[6]

Successful exploitation of third-party vendor cybersecurity vulnerabilities can also compromise critical systems and data and disrupt port operations. In 2020, the U.S. Coast Guard issued a safety alert warning of a cyberattack that exploited a vulnerability in a third-party software application used by a maritime facility. The attack resulted in a ransomware infection that impacted the facility's access control and camera systems, potentially compromising port security. More significantly, in 2018, a phishing email sent to a third-party vendor at the Port of San Diego compromised the port's infrastructure, resulting in the disruption of several critical systems, including the port's IT network, public safety systems, and cargo operations.[7]

The cyber threat to the U.S. MTS is varied and extensive, with possible impacts on local, regional, and national supply chains. And in response, there has been an increase in information sharing regarding cyber threat indicators and related mitigation information (i.e., ransomware, phishing, DDoS, credential stealing, etc.), ultimately leading to the creation of the Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC), the investment in and expansion of USCG Cyber Protection Teams, and the creation of new USCG cyber specialist ratings.

Initially tasked with identifying and assessing the risks of foreign influence in U.S. ports, the

[6] (TLP:WHITE) | CISA | December 2020 | Port Facility Cybersecurity Risks | Infographic | https://www.cisa.gov/sites/default/files/publications/port-facility-cybersecurity-risks-infographic_508.pdf
[7] (U) San Diego Reader | 2019-04-10 | What happened in ransomware attack on Port of San Diego: Iron-backed hackers demand Bitcoin | Online News Article | https://www.sandiegoreader.com/news/2019/apr/10/city-lights-happened-ransomware-port-san-diego/

2023 AEP U.S. Maritime Trade and Port Cybersecurity team's research and analytic outreach resulted in the following findings: (1) a review of how the U.S. MTS is vulnerable to potential physical and cybersecurity threats originating from foreign adversaries using equipment constructed or otherwise controlled by foreign adversaries, and (2) the increased threat of data exfiltration from port community systems (used to exchange information between organizations operating within the same port environment and increase efficiency) and potential delays or disruptions to the MTS.

SHANGHAI ZHENHUA HEAVY INDUSTRIES COMPANY LIMITED (ZPMC) CASE STUDY

Worldwide, maritime ports, facilities, and infrastructure are vulnerable to physical and cybersecurity exploitation by foreign adversaries' (defined in the Office of the Director of National Intelligence's (ODNI) 2023 Annual Threat Assessment) unauthorized access to port equipment and supply chain information management systems. Specifically, foreign adversaries may intentionally introduce vulnerabilities in the port equipment they manufacture, install, and/or otherwise maintain. Such vulnerabilities may pose a significant threat to national and global maritime infrastructure information technology (IT) and operational technology (OT) systems.[8] If these vulnerabilities are exploited, they may result in a breach of confidentiality, integrity, and/or availability of such systems. In turn, this may cause significant monetary losses, result in significant downtime, and threaten national and/or global security.

In April 2022, National Counterterrorism, Innovation, Technology, and Education Center (NCITE) researchers within the DHS Center of Excellence noted that ports are becoming increasingly interconnected, relying more on a physical-cyber infrastructure. A successful cyberattack may result in real-world kinetic effects (i.e., real-world consequences). For example, a successful cyberattack may physically disable or otherwise disrupt port operations (e.g., crane operation disruption and/or delays in port turnaround times) and/or damage electric infrastructure. Such an event may cause a disruption lasting several days to several months.[9]

Shanghai Zhenhua Heavy Industries Company Limited (ZPMC), a subsidiary of China Communications Construction Co. (CCCC), is a primary contractor for Chinese leader Xi Jinping's Belt and Road Initiative to develop infrastructure and trade links across Asia, Africa, and beyond.[10] In 2020, U.S. authorities limited five CCCC subsidiaries' access to U.S.

[8] (U) | US DOT Maritime Administration | 2023-02-17 | 2023-002-Worldwide-Maritime Port Vulnerabilities - Foreign Adversarial Technological, Physical, and Cyber Influence | Advisory | https://www.maritime.dot.gov/msci/2023-002-worldwide-maritime-port-vulnerabilities-foreign-adversarial-technological-physical

[9] (U) | Malone, Iris; Strouboulis, Anastasia; and National Counterterrorism Innovation, Technology, and Education Center, "Emerging Risks in the Marine Transportation System (MTS), 2001- 2021" (2022). Reports, Projects, and Research. 27. https://digitalcommons.unomaha.edu/ncitereportsresearch/27

[10] (U) | Wall Street Journal | Pub 2023-03-05 | Pentagon sees giant cargo cranes as possible Chinese spying tools | Online News Article | https://www.wsj.com/articles/pentagon-sees-giant-cargo-cranes-as-possible-

technology (ZPMC was not on the list), citing its role in Beijing's military-civil fusion program, among other factors. Concurrently, ZPMC equipment enjoys a 70 percent global market share, is utilized in over 100 countries, and makes nearly 80 percent of the cranes used at U.S. ports.

National security and Pentagon officials were reportedly reviewing vulnerabilities linked to ship-to-shore cranes made by ZPMC. Among the concerns was the potential for remotely accessing and controlling the heavy-duty lifting equipment and likely disrupting U.S. logistical operations. Additionally, the cargo cranes are reportedly delivered to the U.S. fully assembled, operated through Chinese-made software, and purportedly, according to a recent report, sometimes managed by Chinese nationals on U.S. visas.[11]

In 2021, according to open-source media reports, the Defense Intelligence Agency (DIA) conducted a classified assessment and found that Beijing could potentially throttle port traffic or gather intelligence on military equipment being shipped. U.S. officials didn't say whether they found any specific instances of ZPMC cranes being used for espionage, however in 2021, FBI agents searched a cargo ship delivering ZPMC cranes to the Baltimore port and found intelligence-gathering equipment on board.[12]

The American Association of Port Authorities (AAPA) has repeatedly highlighted that despite the "sensationalized claims" there is no evidence of the cranes being used to harm or track port operations. AAPA also emphasized the software undergoes rigorous security inspections with federal government partners, it is largely developed by companies in Japan and Sweden, and the cranes do not track the origin, destination, or nature of the cargo.[13] Additionally, 2023 AEP project participants and interview data indicated significant challenges in limiting U.S. domestic use of ZPMC crane equipment based on the national footprint, investment, and procurement time associated with ZPMC cranes.[14] Specifically, research highlighted a primary concern related to the production and delivery of ZPMC cranes:

> "Cranes are delivered to the port **fully assembled with the requested specs, including the operating software**. Essentially, the **cranes are transported from China to U.S. ports ready to be plugged in and begin operating**."—Interview of a U.S. port partner by AEP team members, May 2023. [15] See Figure 3 of a ZPMC crane delivery.

chinese-spying-tools-887c4ade?reflink=desktopwebshare_permalink

[11] (U) | Newsweek | Pub 2023-03-06 | China Accuses U.S. of Paranoia Over Spy Cranes Concern | Online News Article | https://www.newsweek.com/china-america-zpmc-cranes-ports-national-security-1785743

[12] (U) | Wall Street Journal | Pub 2023-03-05 | Pentagon sees giant cargo cranes as possible Chinese spying tools | Online News Article | https://www.wsj.com/articles/pentagon-sees-giant-cargo-cranes-as-possible-chinese-spying-tools-887c4ade?reflink=desktopwebshare_permalink

[13] (U) | The Maritime Executive | Pub 2023-05-19 | US House Bill Seeks to Ban Use of Foreign-Manufactured Cranes in Ports | Online News Article | https://maritime-executive.com/article/us-house-bill-seeks-to-ban-use-of-foreign-manufactured-cranes-in-ports

[14] (U) | 2023 AEP U.S. Maritime Trade and Port Cybersecurity team

[15] (U) | 2023 AEP U.S. Maritime Trade and Port Cybersecurity team

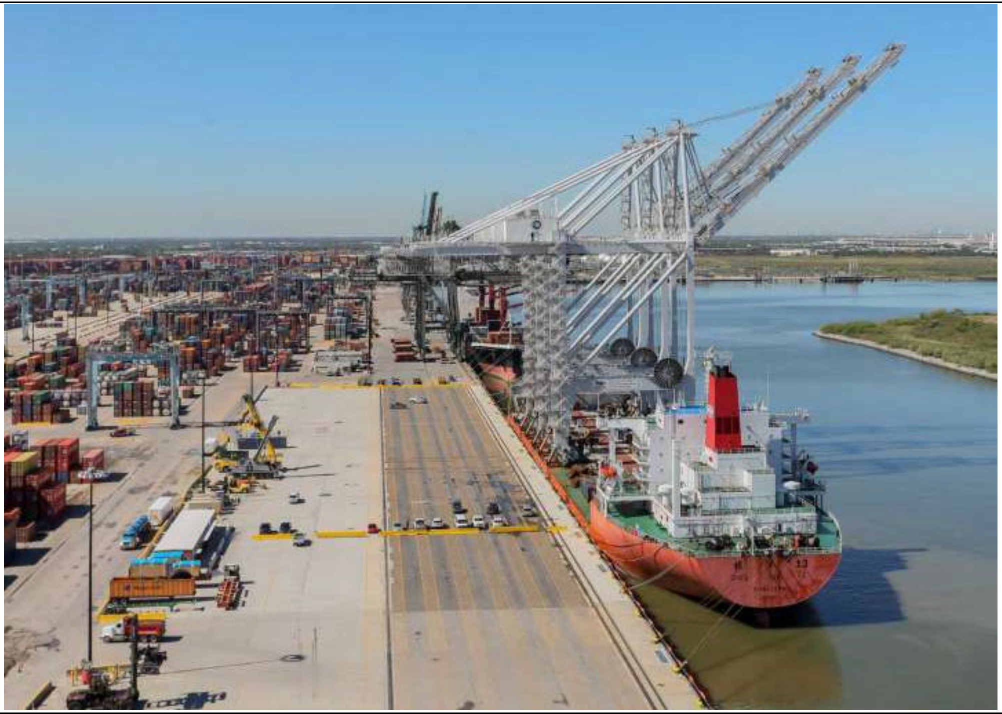


Figure 3. Heavy load carrier ZHEN HUA 13 delivers ZPMC cranes to a port terminal in Houston, TX.[16]

U.S. legislators also summarized this potential concern in an April 2023 letter to the Secretary of Homeland Security, characterizing ZPMC as operating under the umbrella of the Chinese state since its conception, noting the company to have rapidly grown as the dominant global manufacturer of ship-to-shore cranes, and posing a significant risk to U.S. homeland security. These security risks include cyberattacks, espionage, and supply chain vulnerabilities due to the shared software and interconnectivity among ZPMC cranes operating at our nation's ports.[17] In May 2023, US House Representatives introduced the Port Crane Security and Inspection Act of 2023,[18] a largely inspection and assessment-focused move, noting:

> "With respect to **newly constructed foreign cranes** procured for use at a United States port determined by the Secretary to be of **high risk to port security or maritime transportation security and that connect to the internet**, the Secretary of Homeland Security shall, acting through the Cybersecurity and Infrastructure Security Agency, before such crane is placed into service at such port, inspect such crane for potential security risks or threats."—ZPMC

[16] (U) | Crane Market | Pub 2021-10-24 | Three ZPMC ship to shore cranes valued @ $33.5M arrive in Port Houston after 3 month journey | News Article | https://cranemarket.com/blog/three-zpmc-ship-to-shore-cranes-valued-33-5m-arrive-in-port-houston-after-3-month-journey/

[17] (U) | Committee on Homeland Security and the Select Committee on the Strategic Competition between the United States and the Chinese Communist Party (Select Committee on China) (Committees) | 10 May 2023 | ZPMC Crane Oversight Letter | Letter to the Honorable Alejandro Mayorkas, Secretary of Homeland Security

[18] (U) | U.S. House of Representatives | 10 May 2023 | H.R.3169 – Port Crane Security and Inspection Act of 2023 | Bill Introduced to the House of Representatives and Referred to the House Committee on Homeland Security

Crane Oversight Letter, Committee on Homeland Security and the Select Committee on the Strategic Competition between the United States and the Chinese Communist Party (Select Committee on China) (Committees), May 2023[19]

The Act further requires security risks or threat assessments to analyze the threat posed by any existing or newly constructed foreign cranes used at a U.S. port and report the same to Congress.[20]

According to open-source reporting and this subcommittee's research, at least 14 U.S. ports use ZPMC cranes, including the Ports of Charleston, Wilmington, and Tacoma (see Figures 4, 5, and 6). The prevalence of these cranes at U.S. ports with strategic, economic, and national security implications, highlights our concerns with introducing foreign technology into U.S. port environments which may result in more exploitable vulnerabilities and increase the attack surfaces at U.S ports.

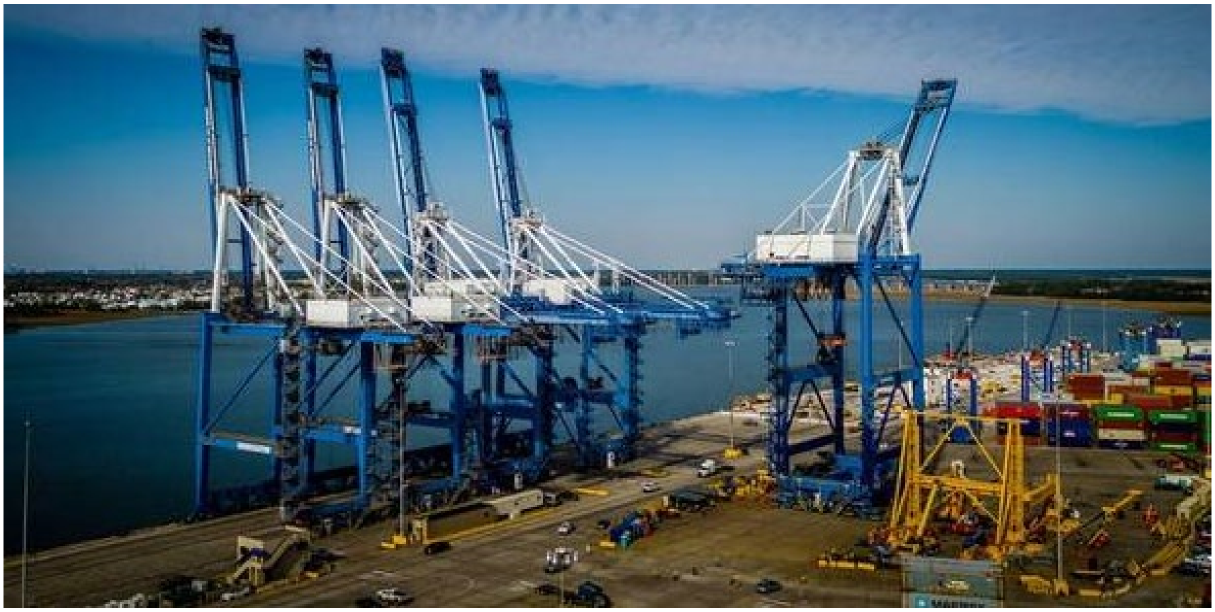


Figure 4. A newly raised ZPMC crane is returning to service after an upgrade in Charleston, SC.[21]

[19] (U) | Committee on Homeland Security and the Select Committee on the Strategic Competition between the United States and the Chinese Communist Party (Select Committee on China) (Committees) | 10 May 2023 | ZPMC Crane Oversight Letter | Letter to the Honorable Alejandro Mayorkas, Secretary of Homeland Security

[20] (U) | U.S. House of Representatives | 10 May 2023 | H.R.3169 – Port Crane Security and Inspection Act of 2023 | Bill Introduced to the House of Representatives and Referred to the House Committee on Homeland Security

[21] (U) | Maritime Professional | Pub 2018-07-11 | ZPMC USA Expands Coast-to-coast | Online News Article | https://www.maritimeprofessional.com/news/zpmc-expands-coast-coast-319480

Figure 5. ZPMC cranes in Wilmington, NC.[22]

[22] (U) | Mfame | Pub 2019-07-22 | Crane Raising To Lift Port Production | Online News Article | https://mfame.guru/crane-raising-to-lift-port-production/

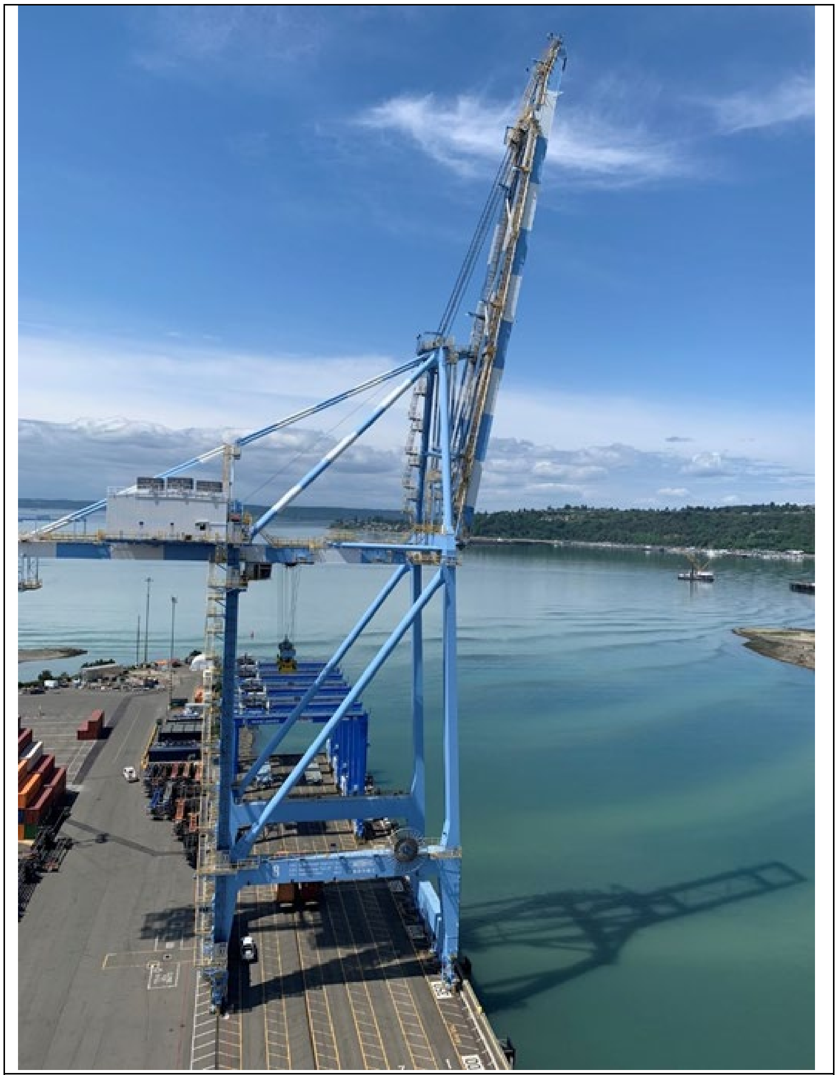


Figure 6. ZPMC crane in Tacoma, WA.[23]

Foreign Investment

There are several open-source examples since the 1990s of the U.S. Government acting to prevent foreign companies from gaining ownership or control over U.S. port operations. The 1998 – 1999 U.S. defense bill blocked COSCO Shipping's attempt to lease a portion of Long Beach (California) Naval Station. In 2006, the U.S. Congress voted to block the proposed purchase by Dubai Ports World (a company based in the United Arab Emirates (UAE)) of the North American terminal and stevedoring operations.[24] [25] In 2018, the U.S. Government again

[23] (U) | Photo taken by AEP Team Member at the Port of Tacoma on 23 May 2023.

[24] (U) | FreightWaves | Pub 2018-04-22 | Foreign investment in U.S. ports face government scrutiny | News Article | https://www.freightwaves.com/news/foreign-investments-in-u-s-ports-face-government-scrutiny?amp

[25] (U) | Council on Foreign Relations | Last Updated 2007-02-13 | Foreign Ownership of U.S. Infrastructure |

intervened to prevent COSCO Shipping from gaining control over the Long Beach Container Terminal at the Port of Long Beach. COSCO Shipping had purchased the Hong Kong-based Orient Overseas International Limited (OOIL) in 2017 for $6 billion. OOIL owned the Long Beach Container Terminal, which operates the Long Beach Container Terminal at the Port of Long Beach.[26] [27]

Despite occasional pushback from U.S. regulators and legislators, foreign entities (especially Chinese ones) exert a high level of economic influence over U.S. ports. COSCO Shipping leases Pacific Container Terminals (Pier J) in the Port of Long Beach through a joint venture it established with SSA Marine in 2001. COSCO Shipping is also a part owner of the company that leases and operates the West Basin Container Terminal in the Port of Los Angeles.[28] Chinese companies also produce or own equipment used at U.S. ports. For example, ZPMC cranes are present in several U.S. ports, including the Ports of Baltimore, Everglades, Houston, Miami, Philadelphia, South Carolina, and Virginia.[29] [30] [31] [32] [33] Non-Chinese entities have also made significant transactions in the U.S. maritime industry; for instance, the Canada Pension Plan Investment Board (CPP Investments) purchased Ports America for $4 billion in September 2021. As of 2023, there are 33 U.S. ports with Ports America-operated terminals, including the Ports of Los Angeles, New York-New Jersey, Savannah, Georgia, and Houston.[34]

Foreign companies are continuing to increase their investments in U.S. ports. At least two proposed transactions are under review by the Committee on Foreign Investment in the United States (CFIUS). The first proposed transaction is a preliminary agreement for the UAE company Gulftainer to lease the Port of Wilmington in Delaware for 50 years and invest $580 million in

Archived Backgrounder | https://www.cfr.org/backgrounder/foreign-ownership-us-infrastructure

[26] (U) | Universal Cargo | Posted 2019-10-15 | U.S. Forces China Out of Port of Long Beach Terminal Ownership | News Blog | https://www.universalcargo.com/u-s-forces-china-out-of-port-of-long-beach-terminal-ownership/

[27] (U) | Newsweek Magazine | Pub 2022-10-09 | China's Stake in World Ports Sharpens Attention on Political Influence | News Article | https://www.newsweek.com/2022/10/14/chinas-stake-world-ports-sharpens-attention-political-influence-1749215.html

[28] (U) | FreightWaves | Pub 2018-04-22 | Foreign investment in U.S. ports face government scrutiny | News Article | https://www.freightwaves.com/news/foreign-investments-in-u-s-ports-face-government-scrutiny?amp

[29] (U) | World Cargo News | Pub 2021-09-14 | Cranes Arrive in Baltimore | News Article | https://www.worldcargonews.com/news/news/cranes-arrive-in-baltimore-67282

[30] (U) | South Florida Sun Sentinel | Pub 2023-04-04 | Chinese cranes at South Florida ports raise security concerns | News Article | https://www.sun-sentinel.com/2023/04/04/lawmakers-fear-cyberspying-from-chinese-made-cranes-in-south-florida-ports/#:~:text=Giant%20gantry%20cranes%20made%20in,for%20interfering%20with%20port%20operations.

[31] (U) | Container Management | Pub 2022-02-11 | Port Houston receives three new neo-Panamax STS cranes | News Article | https://container-mag.com/2022/02/11/port-houston-receives-three-new-neo-panamax-sts-cranes/

[32] (U) | PhilaPort | Pub 2017-12-01 | PhilaPort Purchases Two New Super Post-Panamax Container Cranes | News Release | https://www.philaport.com/philaport-concludes-purchase-of-super-post-panamax-cranes/

[33] (U) | Associated Press | Pub 2019-01-07 | Port: Largest shipping cranes to operate in US have arrived | News Article | https://apnews.com/article/37027c69c06e4fe9af22fb39d54ac0f2

[34] (U) | FreightWaves | Pub 2021-11-09 | US regulators balk at billion-dollar takeover of Ports America | News Article | https://www.freightwaves.com/news/us-regulators-balk-at-billion-dollar-takeover-of-ports-america

the port. The second proposed transaction is a signed letter of intent between the Mississippi State Port Authority and the Turkish company Yilport Holding to discuss future port expansion and a lease.[35]

PORT COMMUNITY SYSTEMS/API CASE STUDY

Port community systems are electronic platforms that support port operations by creating an environment that integrates and streamlines information exchanges between participating private and public port entities, thereby increasing efficiency and promoting ease of business. As operations begin to automate, ports will rely increasingly upon application programming interfaces (APIs) and electronic data interchanges (EDIs) to facilitate that transition. Unauthorized access to port community systems would likely enable adversaries to collect large sets of data on the U.S. supply chain and potentially provide the ability to delay/disrupt the MTS.[36] [37]

Like ports, port community systems are all unique in the services offered, tailored to best support the operations conducted at a port facility. Several common services include terminal control, container status reporting, and scheduling/booking requests and confirmations. Specifically, these systems often incorporate APIs and EDIs that facilitate the multi-directional flow of data between disparate software applications used by organizations conducting business with the port (i.e., rail or trucking) (see Figure 7).[38] [39] In the maritime context, APIs and EDIs allow the port and other entities to share detailed logistical data, thereby increasing interoperability within the supply chain. The emergence of port community systems throughout the industry demonstrates the importance of frictionless data exchange and greater visibility.

[35] (U) | FreightWaves | Pub 2018-04-22 | Foreign investments in Us. Ports face government scrutiny | News Article | https://www.freightwaves.com/news/foreign-investments-in-u-s-ports-face-government-scrutiny

[36] (U) | International Association of Ports and Harbors (IAPH) Trade Facilitation and Port Community Systems Committee | Pub June 2011 | Port Community Systems Benchmark Survey | A Report on Benchmark Survey Results

[37] (U) | Notteboom, Theo; Pallis, Athanasios; and Rodrigue, Jean-Paul | 2022 | Port Economic, Management and Policy, II. Contemporary Ports, Chapter 2.4—The Digital Transformation of Ports: Port Community System | doi.org/10.4324/9780429318184

[38] (U) | According to open-source reporting, eventually, EDIs will be replaced by APIs.

[39] (U) | Notteboom, Theo; Pallis, Athanasios; and Rodrigue, Jean-Paul | 2022 | Port Economic, Management and Policy, II. Contemporary Ports, Chapter 2.4—The Digital Transformation of Ports: Port Community System | doi.org/10.4324/9780429318184

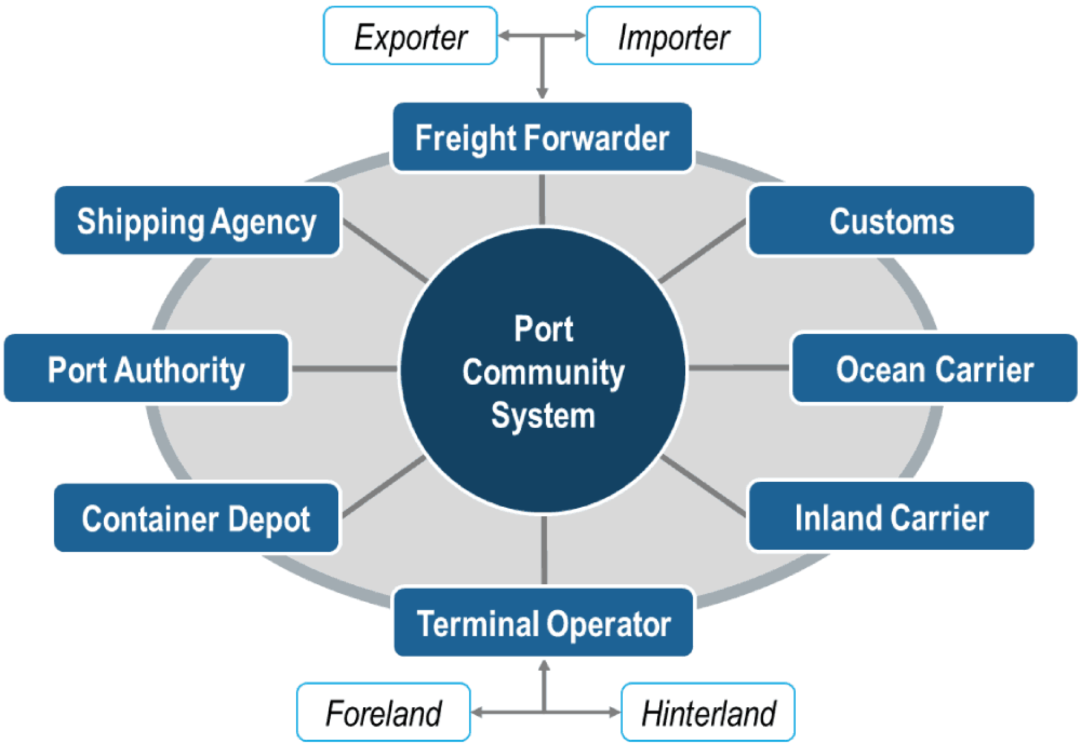


Figure 7. An example of a port community system and its various connections.[40]

As the connector between disparate systems, APIs should incorporate basic cybersecurity measures to protect the data it shares, even when the exchange occurs within a port community system. Despite the anticipated increase in API usage—APIs are expected to approach 1.7 billion by 2030[41]—and the use of REST APIs as a best practice, the structure of APIs remains unregulated and unstandardized, and not all APIs are designed with security in mind. Insecure APIs make the supply chain vulnerable to data leaks.[42] In 2022, U.S. companies suffered a reported $12 billion to $23 billion in losses from compromises caused by leaky or otherwise insecure APIs, according to a report on open-source breach data.[43] In 2021, several high-profile API security incidents include the Parler platform data harvest, Microsoft Exchange Server attacks coordinated by a Chinese state-sponsored hacking group, and the widespread Log4j vulnerability.[44]

[40] (U) | Notteboom, Theo; Pallis, Athanasios; and Rodrigue, Jean-Paul | 2022 | Port Economic, Management and Policy, II. Contemporary Ports, Chapter 2.4—The Digital Transformation of Ports: Port Community System | doi.org/10.4324/9780429318184
[41] (U) | DevOps | Pub 2021-12-07 | API Sprawl a Looming Threat to Digital Economy | Online News Article | https://devops.com/api-sprawl-a-looming-threat-to-digital-economy/
[42] (U) | OWASP | Accessed on 2023-07-25 | “OWASP API Security Project – OWASP Foundation” | Webpage | https://owasp.org/www-project-api-security/
[43] (U) | Dark Reading | Pub 2022-06-30 | API Security Losses Total Billions, But It’s Complicated | Online News Article | https://www.darkreading.com/application-security/api-security-losses-billions-complicated
[44] (U) | Salt Security | 2021-12-21 | Recap: The 7 Biggest API Security Incidents in 2021 | Security Blog | https://salt.security/blog/recap-7-biggest-api-security-incidents-in-2021

According to a recent article, the eModal platform is the world's largest port community system serving intermodal operators in North, Central, and South America, Australia, and the United Kingdom.[45] According to the company's website (as shown in Figure 8), eModal is said to be widely used by North American container terminals to manage truck-tracking and landside performance, environmental programs, traffic mitigation, fee collection, and appointment and pre-arrival solutions to drive gate and cargo velocity. The eModal platform is reported to use APIs to facilitate the exchange of cargo and information between port facilities and stakeholders. The eModal Data Services API is also reported to increase port operation transparency through real-time connections to terminal operating systems, enabling third-party logistics companies, such as trucking and shipping companies, to have end-to-end visibility of cargo, predictive cargo availability, and the capability to schedule terminal appointments.[46] [47]

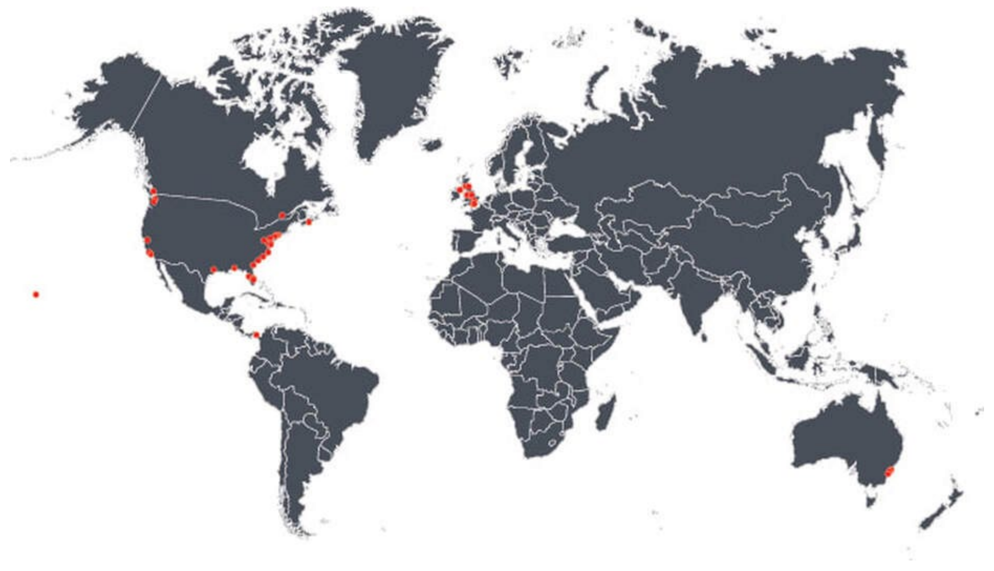


Figure 8. eModal Product Usage.[48]

As of 2023, open-source reporting indicates malicious cyber actors have targeted port community systems. In July 2023, malicious cyber actors deployed ransomware to infect the port community system (Nagoya United Terminal System [NUTS]) at the largest port in Japan,

[45] (U) | Business Wire | Pub 2021-12-01 | eModal Assists Medical Suppliers with "Fast Track" Digital Processing for Import Container Pickups: A Streamlined Path for Medical Supplies to Bypass Port Congestion | Online News Article | https://www.businesswire.com/news/home/20211201005286/en/eModal-Assists-Medical-Suppliers-with-%E2%80%9CFast-Track%E2%80%9D-Digital-Processing-for-Import-Container-Pickups

[46] (U) | Advent eModal | Pub 2019-03-05 | eModal Data Services (EDS) | YouTube Video | https://www.youtube.com/watch?v=Krtv6vfeuXw

[47] (U) | Advent eModal | Pub 2019-05-05 | eModal Community Portal | YouTube Video | https://www.youtube.com/watch?v=ZSFD5i1FXSQ&t=14s

[48] (U) | Advent eModal | Accessed on 2023-07-15 | "Advent eModal – Advent eModal Overview" | Webpage | https://www.adventemodal.com/

Port of Nagoya, stopping all container movements.[49] As of July 2023, information on how the system was compromised had not been released; however, the incident demonstrates a capability and intent to target port community systems.[50] With the widespread use of the eModal platform at U.S. port complexes, the recent targeting of a port community system and the impacts on port operations is very concerning.[51] Additionally, the incident highlights the criticality of a port community system to the continuity of port operations.[52] [53]

Port community systems may also be used by foreign adversaries looking to gain a competitive edge. Beyond eModal, other port community systems include the French-based system SOGET, the Chinese-based system LOGINK, and the Dutch-based system Portbase.[54] Of the three, LOGINK is the second most used port community system, with the Chinese state-sponsored and -supported platform partnering with over 20 ports and numerous international companies. China's government aims to expand the platform's presence by providing freight carriers, forwarders, and entities operating at ports worldwide free access to the system.[55]

In September 2022, the U.S.-China Economic and Security Review Commission found widespread adoption of LOGINK could create economic and strategic risks for the U.S. and other countries by giving China a competitive edge. According to the issue brief, the overall security of the state-funded platform is unclear, and the Chinese government may use the system to access and control sensitive business and foreign government data. Through LOGINK's visibility of aggregated global commercial data, the Chinese government could identify vulnerabilities within the U.S. and global supply chain and use gleaned information "to expand and more precisely target [economic competitors with] its use of economic coercion" (i.e., sanctions). In addition, LOGINK could be used to track the transportation of military cargo via commercial logistic companies, providing Chinese military planners with trends and early warnings of force projection movements.[56]

[49] (U) | International Association of Ports and Harbors (IAPH) Trade Facilitation and Port Community Systems Committee | Pub June 2011 | Port Community Systems Benchmark Survey | pg. 3 | A Report on Benchmark Survey Results

[50] (U) | Security Magazine | Pub 2023-07-06 | Experts discuss cyberattack at Japan's largest port | Online Article | https://www.securitymagazine.com/articles/99601-experts-discuss-cyberattack-at-japans-largest-port#:~:text=According%20to%20reports%2C%20container%20operations,to%20a%20pro%2DRussian%20group.

[51] (U) | Advent eModal | Accessed on 2023-07-15 | "Advent eModal – Advent eModal Overview" | Webpage | https://www.adventemodal.com/

[52] (U) | TechRadar | Pub 2023-07-05 | Japan's busiest port shut down by ransomware attack: Nagoya port forced to close operations for several days | News Article | https://www.techradar.com/pro/japans-busiest-port-shut-down-by-ransomware-attack

[53] (U) | BleepingComputer | Pub 2023-07-05 | Japan's largest port stops operations after ransomware attack | Online News Article | https://www.bleepingcomputer.com/news/security/japans-largest-port-stops-operations-after-ransomware-attack/

[54] (U) | International Port Community Systems Association (IPCSA) | Accessed on 2023-07-15 | "Members – IPCSA International" | Webpage | https://ipcsa.international/about/members/

[55] (U) | U.S.-China Economic and Security Review Commission | 2022-09-20 | LOGINK: Risks from China's Promotion of a Global Logistics Management Platform | Issue Brief.

[56] (U) | U.S.-China Economic and Security Review Commission | 2022-09-20 | LOGINK: Risks from China's

OTHER CONCERNING IMPACTS TO THE PUBLIC SECTOR

There are additional significant national security implications if the above vulnerabilities are not mitigated. According to the U.S. Department of Transportation (DOT) Maritime Administration (MARAD), there are 18 privately owned ports used for national security initiatives as part of the National Port Readiness Network. Of the 18 commercial seaports, several conduct container operations using ZPMC cranes. See Figures 9 and 10 for the ports involved in the National Port Readiness Network.[57]

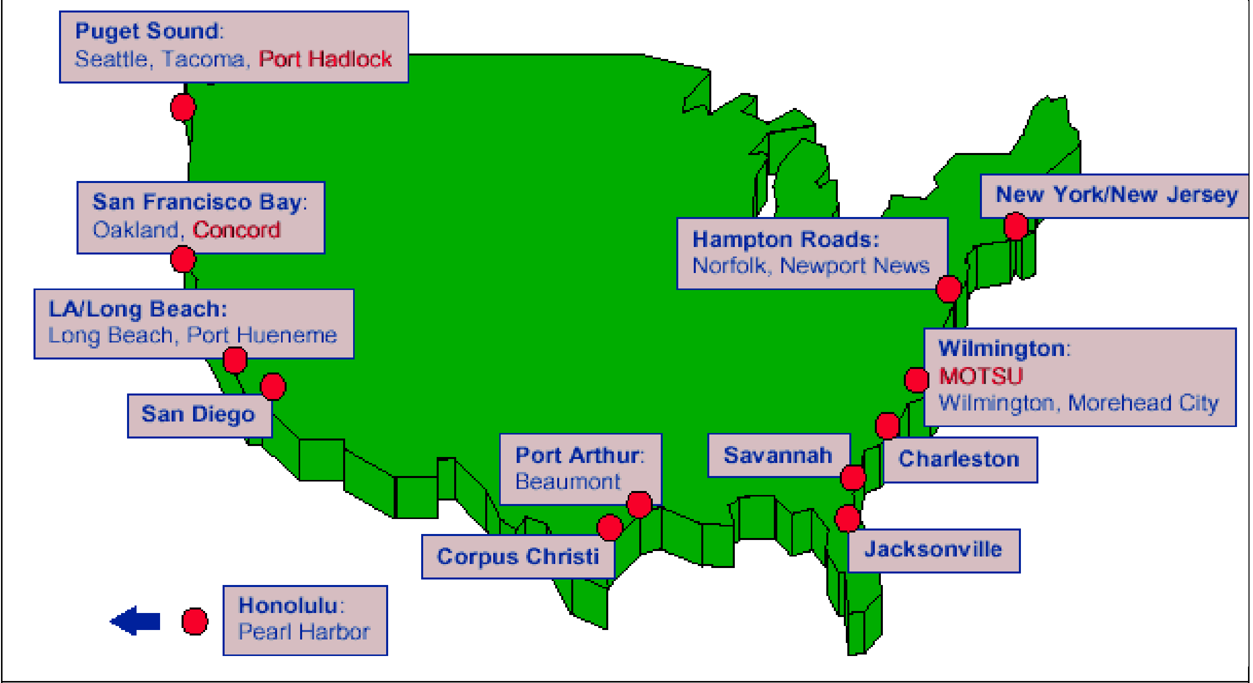


Figure 9. Map of the Commercial Strategic Ports.[58] [59]

Promotion of a Global Logistics Management Platform | Issue Brief.

[57] (U) | U.S. Department of Transportation Maritime Administration | Accessed on 2023-07-20 | "National Port Readiness Network (NPRN) – MARAD" | Webpage |https://www.maritime.dot.gov/ports/strong-ports/national-port-readiness-network-nprn

[58] (U) | GlobalSecurity.org | Accessed on 2023-07-20 | "National Port Readiness Network" | Webpage |https://www.globalsecurity.org/military/agency/dot/nprn.htm

[59] (U) | U.S. Department of Transportation Maritime Administration | Accessed on 2023-07-20 | "National Port Readiness Network (NPRN) – MARAD" | Webpage |https://www.maritime.dot.gov/ports/strong-ports/national-port-readiness-network-nprn

Anchorage, AK	Gulfport, MS	Philadelphia, PA
Beaumont, TX	Hampton Roads, VA	Port Arthur, TX
Charleston, SC	Jacksonville, FL	San Diego, CA
Corpus Christi, TX	Long Beach, CA	Savannah, GA
Port of Everett, WA	Morehead City, NC	Tacoma, WA
Port of Guam, GU	Oakland, CA	Wilmington, NC

Figure 10. List of Commercial Strategic Ports.[60] [61]

RECOMMENDATIONS

Regulations and Relationships – The Need for Partnership

Based on survey information and interviews with subject matter experts, additional oversight and partnerships could significantly enhance the security of U.S. ports and the maritime transportation system (MTS). This subcommittee has gathered the following recommendations to begin the dialogue on better securing the MTS.

- **Streamline and update regulations:** Potential benefit exists to coordinate and update federal regulations across current oversight mechanisms to enable the port operator to require minimum standards of tenants or companies operating in the port to create a more secure environment and improve the overall port cybersecurity. Enabling the USCG to regulate and enforce these expanded regulations would effectively consolidate the reporting and oversight functions within the sector. Other sectors of the U.S. economy are ahead of the maritime industry, like the utility industry with NERC-CIP and some federal agencies with FedRamp and CMMC. Minimum standards for infrastructure management should also include API security. Potential further regulatory opportunities toward standardization include:
    - **Conduct Annual Risk Assessments and Audits.** Port operators should conduct regular risk assessments and audits of their cybersecurity posture, including third-party risk audits of companies trading in their port ecosystem. This includes identifying and assessing potential vulnerabilities, evaluating existing security controls' effectiveness, and prioritizing improvement areas. Companies can implement targeted cybersecurity measures to protect their operations, systems, and data by understanding their unique risk landscape.
    - **Implement Robust Access Control and User Management.** Port operators

[60] (U) | GlobalSecurity.org | Accessed on 2023-07-20 | "National Port Readiness Network" | Webpage |https://www.globalsecurity.org/military/agency/dot/nprn.htm
[61] (U) | U.S. Department of Transportation Maritime Administration | Accessed on 2023-07-20 | "National Port Readiness Network (NPRN) – MARAD" | Webpage |https://www.maritime.dot.gov/ports/strong-ports/national-port-readiness-network-nprn

should enforce strong access controls and systems-driven user management practices within the port ecosystem. This involves implementing the principle of least privilege, where employees, contractors, and others are granted only the minimum level of access required to perform their duties. Additionally, companies should enforce strong password policies, including complex passwords, regular password changes, multi-factor authentication (MFA) for critical systems, or even passwordless authentication configurations.

  - **Develop Robust Incident Response and Business Continuity Plans.** Port operators and companies operating in the port footprint should be required to develop comprehensive incident response plans (IRPs), business continuity plans (BCPs), and disaster recovery plans (DRPs) to address cybersecurity incidents, ensure the continuity of operations, and have appropriate disaster recovery plans. IRPs outline the step-by-step procedures to detect, respond to, and recover from cyber incidents. At the same time, BCPs provide guidelines for maintaining essential services and operations during and after an incident. DRPs document the procedures of recovering from a physical or manmade (i.e., cyber or otherwise) disaster. Regularly testing and updating these plans, conducting tabletop exercises, and training employees on their roles and responsibilities will ensure an effective response to cybersecurity incidents and minimize downtime.

- **Foster partnerships and information sharing:** Port operators should actively engage in partnerships and information-sharing initiatives within the port community. This includes collaborating with port authorities, other commercial entities, and government agencies to share threat intelligence, best practices, and lessons learned. By participating in industry forums, cybersecurity working groups, and information-sharing platforms, companies can stay informed about emerging threats and adopt proactive measures to enhance their cybersecurity defenses. Potential opportunities for partnership engagement include the following:

  - **Regional SOCs.** Consider the creation of regional Security Operations Centers (SOCs) to monitor endpoint and network traffic for all port and maritime entities in the region. Joining a SOC would be at the discretion of each company but may be incentivized through priority engagement activities that allow the SOC to provide a managed detection and response of all member SOC companies to allow visibility to attempted intrusions and anomalous activities and inject data from IAM and vulnerability management systems.

  - **Formalized Information Sharing.** Harness processes through engagement and membership of information sharing and analysis centers (ISACs) such as the Multi-State ISAC (MS-ISAC) and the Maritime Transportation System (MTS-ISAC) to receive timely information (in the form of threat intelligence and actionable alerts) to improve industry's cybersecurity posture and build a more robust cyber defense community.[62] [63] Subsidize membership fees and connect with the National Network of Fusion Centers and the local USCG Area Maritime Security Committees to facilitate information flow and intelligence production across the national MTS landscape.

- **Shared Continuous Attack Surface Management System.** Given the multitude of logistics partners operating in port facilities, it is likely that even with minimized attack surfaces within the port facilities' networks, attackers could gain access through third-party entities. To accurately assess the scope of such threats, port facilities extending to companies operating in the port footprint need to perform detailed network mapping and identify on a continuous basis all the potential third-party entities that may access a port facility's network. The monitoring would be most effective if done on a shared basis.

- **Active Threat Assessments.** Using the detailed network mapping information, the port facilities and companies operating in the port footprint can then perform open-source searches on trusted platforms to identify which third-party networks have significant attack surfaces that could allow malicious cyber actors access to the third-party networks and indirect access to the port facilities' networks. Such analysis is beyond the scope of this report but would be highly beneficial for individual facilities to conduct. This subcommittee also recommends that port facilities look to adopt a zero-trust maturity model, which includes deploying network segmentation to determine which areas of the network should be isolated or otherwise contained to mitigate threats such as unwanted data exfiltration, the spread of ransomware, and more.[64] [65]

- **Invest in training and awareness:** Companies operating within the port footprint should prioritize cybersecurity training and awareness programs for their employees and contractors. Training should cover topics such as identifying phishing emails, recognizing social engineering techniques, and reporting suspicious activities. Regular awareness campaigns that simulate phishing exercises and ongoing education will help create a security-conscious workforce that actively contributes to a company's cybersecurity defenses.

> "The concern is the coordinated attacks against similar entities, performing similar functions, likely having similar computer systems and consequently similar vulnerabilities. In a port community, similar entities exist throughout the ecosystem. A coordinated attack against multiple entities in the ecosystem could cut off the flow of goods at a port and disrupt the entire community - and indeed national economies and international trade - by breaking the

[62] (U) | MS-ISAC | Accessed on 2023-07-26 | "MS-ISAC" | Webpage | https://www.cisecurity.org/ms-isac
[63] (U) | MTS-ISAC | Accessed on 2023-07-26 | "MTS-ISAC" | Webpage | https://www.mtsisac.org
[64] (U) | CISA | Accessed on 26 July 2023 | "Zero Trust Maturity Model | CISA" | Webpage | https://www.cisa.gov/zero-trust-maturity-model
[65] (U) | Microsoft | Accessed on 26 July 2023 | "Evaluate your Zero Trust security posture" | Webpage | https://www.microsoft.com/en-us/security/business/zero-trust/maturity-model-assessment-tool?activetab=solution-wizard:primaryr1

supply chain. **The most effective countermeasure to a coordinated cyberattack is a coordinated cyber defense by the port community.**"—Port Community Cyber Security, World Ports Sustainability Program, June 2020[66]

- **Develop a plan to address open APIs across the Port Community Ecosystem:** Unlike maritime infrastructure that falls under the Maritime Transportation Security Act of 2002 (MTSA), 46 U.S.C. 70101 et seq., port community systems and APIs are not regulated, nor do they fall under any minimum cybersecurity standards. As such, insecure APIs/EDIs may go unaddressed and connect to port community systems, potentially allowing unauthorized data exfiltration and system disruptions by foreign adversaries looking to gain a competitive edge. The APIs used by multiple strategic ports could be a single point of failure if the API is not secured properly, and organizations should take inventory of existing APIs and assess the risk each poses. Consideration should be given to addressing this tactical-strategic issue, potentially through the assistance of the MTS-ISAC, while evolving the system as a whole.

IMPACTS OF THE RECOMMENDATIONS

The Maritime Transportation System (MTS) has long served as the backbone of global trade, connecting ports and facilitating commerce. The current evolutions in the cybersecurity threat environment have occurred at a faster rate than the speed in which regulatory norms, common best practices, and increasing reliance on technology for trade. Regardless, any recommended change needs to be assessed, considering the pragmatic need for trade matched with appropriate cybersecurity measures.

Streamlining regulations and standards holds the potential for economic and operational enhancements and can ultimately speed trade and make it more secure. Consolidating disparate regulatory requirements and clarifying specific minimum standards could drastically reduce compliance costs fostering market accessibility and accelerating business transactions. Nonetheless, harmonization necessitates careful negotiation, balancing simplification with maintaining stringent safety and security standards like those implemented in the Maritime Transportation Security Act.

Regional Security Operations Centers (SOCs) are poised to play an even more critical role. The cost of every trading partner in the port ecosystem maintaining a separate SOC with appropriate visibility is far greater than the shared SOC designed to support many. Their potential for contextualized threat intelligence, rapid incident response, and bolstered regional cybersecurity can directly improve business speed. However, synchronizing activities across SOCs, ensuring resource allocation, and establishing clear channels of communication will be crucial to prevent overlaps and gaps.

[66] (U) | World Ports Sustainability Program | Pub June 2020 | IAPH Port Community Cyber Security | Report | https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf

In parallel, formalizing information sharing in port and maritime operations promises to optimize risk assessment and stimulate innovation. Establishing standardized protocols can expedite decision-making and reduce costs associated with managing information security. However, the implementation must address potential data privacy concerns and the balance between transparency and competitive advantage.

Finally, open APIs in the MTS ecosystem, on the one hand, have greatly improved the ability of companies to trade, but, on the other hand, if left unregulated, create a clear and evident risk to the destruction of the system as known from near unfettered exfiltration of data and the system being used a highly efficient asset by an adversary. This report recognizes the cost of converting to secure APIs, as well as the cost of maintaining those secure APIs, which will demand substantial resources. However, left unattended, the MTS is difficult, if not impossible, to secure.

The future landscape of port and maritime operations appears complex yet ripe with opportunities. As the United States navigates the challenges and updates how it addresses cybersecurity, the reward is a more efficient, resilient, and secure MTS for the global community. However, it is pivotal to continually assess and adapt to the ever-evolving technological, regulatory, and operational landscape of the maritime sector and the continued discussion of how to address the shared responsibility of the public-private partnership for increased cybersecurity in the port and maritime environment.

AREAS FOR FUTURE STUDY

Emerging technologies, such as artificial intelligence, ship and fleet management systems, and increased automation through internet-connected devices, hold the promise for transforming port operations and enhancing supply chain visibility. However, adopting these technologies introduces new cybersecurity vulnerabilities that must be carefully assessed and mitigated. Additionally, some new technologies rely heavily, if not exclusively, on foreign supply chains to deliver such capabilities to U.S. ports. The potential exploitation of AI-enabled systems, the unknown security of ship and fleet management systems, and unauthorized access to connected devices are some areas of future concern.

The Impact of AI on Port and Maritime: While artificial intelligence (AI) systems are being developed and deployed in the port environment, if not appropriately secured, they may provide an open door to malicious actors. Preliminary research has indicated that AI can be easily fooled into mistaking objects or misreading data. Examples include wearing markings on one’s face or clothes to cause the algorithm to identify a person as an inanimate object or placing markings on street signs such as speed limit postings that cause AI in vehicles to incorrectly interpret the speed limit to something significantly higher, posing a danger to pedestrians and vehicle occupants.[67] These types of tactics could be readily implemented in the maritime domain, with ship's utilizing such markings to mask cargo or the ship itself while at sea or to disrupt container port operations by causing errors within automated cranes.[68]

AI also presents a challenge by enabling malicious cyber actors to develop scripts that could allow for complex attacks on facilities. AI could also potentially be used to improve target identification and reconnaissance, eliminating the antiquated but frequently used concept of "security through obscurity." Given the potential capabilities of AI, malicious actors could craft tailored attacks against specific facilities, vendors, or ships in a fleet, possibly without the target identifying the attack in a timely manner. At a minimum, AI will likely increase the ability of malicious actors to automate tasks that allow for the increased efficacy of cyberattacks.[69]

Ship and Fleet Management Systems: Another area of concern is the growing market for ship and fleet management systems. These systems are designed to automate various shipboard operational and administrative processes, from managing the steering and propulsion systems to sending out notice of arrival documents to port officials. Like the challenges currently faced by port facilities, this increased automation potentially provides new attack vectors for malicious actors. In January 2023, the Norwegian shipping registrar and classification agency DNV suffered a cyberattack on its ShipManager and Navigator systems, which provide fleet management automation services, affecting over a thousand vessels operated by several hundred companies. As of July 2023, DNV provided scant details about the January cyberattack, highlighting the general approach of private sector industries of not sharing significant information about attacks that could serve as lessons learned for competitors to better secure their own products.

Depending on the level of automation and interconnectivity to other systems, ship and fleet management systems could potentially provide another vector of cyberattacks for port facilities as well. With some systems managing compliance procedures, such as sending out notice of arrival information and other documents required by a port, attacking and breaching such systems may provide attackers a means of then attacking specific port facilities. Additionally, such systems will likely provide malicious cyber actors with significant amounts of information about a shipping company's operations that could be used for further attack reconnaissance, provided to nation-state actors for further cyber espionage, or targeted for ransomware attacks. The evolution of such technologies will require close monitoring to ensure the incorporation of sufficient cybersecurity measures into the product via the "secure-by-design" methodology.

[67] (U) | Comiter, Marcus | August 2019 | Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It. | Harvard Belief Center Paper

[68] (U) | The White House | Pub. 2023-07-21 | FACT SHEET: Biden-Harris Administration Secures voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by Ais.

[69] (U) | Brundage, Avin, Clark, Tonner, and Eckersley | February 2018 | The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.

Interconnected devices: A final area of concern is that of Internet-connected devices, sometimes referred to as Internet-of-Things (IoT) devices, and their potential for increasing the attack surface of a network. While the idea of these devices presenting vulnerabilities is not new, the types of devices that may connect to the internet in the future are the focus of this concern. Within port facilities and on board ships, the inclusion of increasing amounts of "smart" technologies that provide some level of internet, Bluetooth, or other forms of communication technologies presents an increasing challenge for adequately securing networks from attacks.[70] This report and others have noted the cybersecurity concerns regarding automated container cranes located within port facilities as an example of a current connected device that could be exploited. In the future, port facilities and ships will need to closely consider the inclusion of other automated operational technology (OT) systems, whether automated shipboard cranes, GPS-connected life rafts, automated weather-diversionary navigation systems, or any other system likely to be developed in the next decade.

Beyond the vulnerabilities of OT systems, facilities and ships will also need to consider the vulnerabilities potentially introduced with other connected devices, such as televisions, office equipment, or medical devices utilized by employees.[71] How these devices connect to various networks, what information they can collect and transmit, and the potential means of exploitation will need to be thoroughly understood by the management of facilities and shipping companies.[72] While port facilities will likely be more directly affected by policies and procedures for introducing connected devices given the current state of technology, shipping companies potentially face much more severe consequences for not taking appropriate steps to mitigate these risks now. Ships have historically been isolated and disconnected while transiting across the seas, and this historical perspective risks lulling shipboard operators into complacency regarding increased connectivity, especially if the fleet managers and shipboard operators are not familiar with the full connective capabilities of new technologies.

While the advent of these new technologies will improve the efficiency of global shipping and ultimately improve the quality of life for the global commons, they also potentially present new vulnerabilities that could have significant consequences if not properly and effectively managed. Future research examining the effects of these technologies on global shipping and port facility cybersecurity will likely provide critical findings for managers and operators alike.

[70] (U) | USTELECOM, The Broadband Association | 2023 | 2023 USTELECOM Cybersecurity Culture Report: The State of Small and Medium-Sized Critical Infrastructure Enterprises | Report | https://ustelecom.org/wp-content/uploads/2023/02/USTelecom-2023-SMB-Cyber-report.pdf

[71] (U) | IMDRF, Medical Device Cybersecurity Working Group | 2023 | Principles and Practices for the Cybersecurity of Legacy Medical Devices | Report | https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices

[72] (U) | OWASP | Accessed on 2023-07-25 | "OWASP Top Ten – OWASP Foundation" | Webpage | https://owasp.org/www-project-top-ten/

OUTLOOK

The outlook of U.S. maritime trade and port cybersecurity will likely remain relatively constant in the short term due to some key factors. This is not to say that progress towards securing ports is not achievable, but that, barring a major cybersecurity catastrophe at a port, such progress will likely be incremental over the next few years. Foreign investment in the U.S. maritime trade sector and port cybersecurity continues to be an area of concern for members of the maritime community, and has increasingly garnered attention from others, such as lawmakers, media, and others. However, despite recent media and Congressional attention on these issues, particularly foreign investment in U.S. port facilities and equipment, at the time of writing, no significant efforts to improve regulation or streamline legislation appear to be on the horizon. The maritime transportation sector will likely continue operating under limited, piecemeal regulations under the auspices of several federal agencies with varied reporting requirements that will likely continue to challenge efforts to enhance communications between the government and industry for the foreseeable future.

The maritime industry also plays a role in continuing the regulatory morass through its opposition to new regulations. While it would behoove the government to engage with industry in discussions about new regulations to solicit its input on the second- and third-order effects, it cannot abdicate its regulatory role simply because industry views regulations as burdensome. Therefore, it is imperative that industry approach such discussions with an acknowledgment that regulation of some form is both needed and of potentially great benefit in both securing port facilities, ships, and third-party vendors, as well as streamlining and improving the reporting and engagement mechanisms with the government. However, the industry's adoption of such mindsets will likely take time, further postponing potentially viable solutions while government and industry find common goals and acceptable solutions.

Meanwhile, while government and industry search for common ground with respect to regulation, foreign nations will continue to use legislative and regulatory processes to gain further footholds in U.S. ports, with some likely looking to exploit such accesses for strategic military or economic purposes. To clarify, not all, and, in fact, most foreign investment directly benefits the U.S. economy. However, balancing the risk-reward equation when it comes to certain foreign actors should be viewed with paramount importance. This balancing act requires meaningful engagement between government and industry.

Beyond foreign investment risks, delayed regulation will also likely directly affect the goal of implementing "secure-by-design" software in port facilities and onboard ships. While both government and leading technology firms have agreed that implementing cybersecurity features in products throughout product development is critical to achieving more secure products, the current economic dynamics still favor speed over security when launching products and bringing them to the market. As such, without some degree of government regulation to force a change in mindsets, it will likely take several years for technology firms to fully embrace security over speed in product development and deployment.

While it is the hope of this subcommittee that the recommendations provided in this report can assist government and industry to rapidly identify and implement regulations and solutions to mitigate those risks presented as well as others, the likelihood is that these challenges, while not intractable, will continue to persist in the coming years. It is often said that if you have seen a port facility, you have only seen *a* port facility. This stems from the unique operations, configurations, cultures, and challenges at each facility, and, at least for the foreseeable future, will also extend into the mitigation approaches for foreign investment and cybersecurity. Instead of implementing an integrated network defense of its port facilities, the U.S. maritime transportation sector will likely continue operating in silos, with each port responsible for its own protection and without an understanding of how its cybersecurity decisions affect the larger U.S. economy, both in relation to other port facilities and as a part of the increasingly connected and networked economic system.

ANALYTIC DELIVERABLE DISSEMINATION PLAN

- National Security Council (NSC)
- American Association of Port Authorities (AAPA)
- National Council of Information Sharing and Analysis Centers (ISACs)
  - Information Technology (IT-ISAC)
  - Maritime Transportation System (MTS-ISAC)
  - Maritime (Maritime-ISAC)
  - Multi-State ISAC (MS-ISAC)
  - National Defense (ND-ISAC)
  - Oil & Natural Gas (ONG-ISAC)
- U.S. Coast Guard (USCG)
  - USCG Cyber Command (CGCYBER)
  - USCG Assistant Commandant for Prevention Policy (CG-5P)
  - USCG Assistant Commandant for Response Policy (CG-5R)
  - USCG Assistant Commandant for Intelligence (CG-2)
  - USCG Commander, Atlantic Area
  - USCG Commander, Pacific Area
- Cybersecurity and Infrastructure Security Agency (CISA)
  - National Infrastructure Coordinating Center (NICC)
  - National Cybersecurity and Communications Integration Center (NCCIC)
- Office of the Director of National Intelligence (ODNI)
  - National Maritime Intelligence-Integration Office (NMIO)
  - Cyber Threat Intelligence Integration Center (CTIIC)
  - National Counterintelligence and Security Center (NCSC)
- Department of Homeland Security (DHS)
  - Office of Intelligence and Analysis (I&A)
  - Customs and Border Patrol (CBP)
  - Transportation Security Administration (TSA)

  - Secret Service Electronic Crimes Task Force (ECTF)
- Department of Energy (DOE)
  - Cybersecurity, Energy Security, and Emergency Response (CESER)
- Department of State (DOS)
  - Bureau of Cyberspace and Digital Policy
  - Bureau of Intelligence and Research (INR)
  - Overseas Security Advisory Council (OSAC)
- Department of the Treasury (DOTT)
  - Office of Cybersecurity and Critical Infrastructure Protection (OCCIP)
  - Office of Intelligence and Analysis (OIA)
- Department of Transportation (DOT)
  - Office of Intelligence, Energy Response, and Security
  - Maritime Administration (MARAD)
- Federal Bureau of Investigation (FBI)
  - Office of Private Sector (OPS)
  - InfraGard
- National Security Agency (NSA)
- Central Intelligence Agency (CIA)
- Committee on Foreign Investment in the United States (CFIUS)
- National Network of Fusion Centers

DISCLAIMER STATEMENT: *This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and the product of joint public and private sector efforts.*