NATIONAL MARITIME CYBERSECURITY PLAN

TO THE NATIONAL STRATEGY FOR MARITIME SECURITY

DECEMBER 2020

My Fellow Americans,

The American people elected me on the promise to make America great again. I promised that I would protect American interests and promote the welfare and economy of our great citizens.

During my first year in office, I designated Transportation and Maritime Sector Cybersecurity as a priority for my Administration. In keeping with my promise and this priority, I am continuing to promote the second pillar of the National Security Strategy, Promote American Prosperity, by approving the National Maritime Cybersecurity plan.

The National Maritime Cybersecurity Plan explains how my Administration will:

- Defend the American economy by establishing internationally recognized measures of risks to the Maritime Sub-Sector and standards to mitigate those risks;
- Promote prosperity through information and intelligence sharing; and
- Preserve and increase our great Nation's cyber workforce

The National Maritime Cybersecurity plan demonstrates my commitment to promoting American prosperity by strengthening our cybersecurity. This is a call to action for ALL NATIONS to join us in protecting the vital maritime sector that interconnects us.

Sincerely,

President Donald J. Trump

The White House
December, 2020

We cannot ignore the costs of malicious cyber activity – economic or otherwise – directed at America's Government, businesses, and private industry.
President Donald J. Trump, 2018

TABLE OF CONTENTS

INTRODUCTION

The Unites States is a maritime Nation consisting of an integrated network of 25,000 miles of coastal and inland waterways, 361 ports, 124 shipyards, more than 3,500 maritime facilities, 20,000 bridges, 50,000 Federal aids to navigation, and 95,000 miles of shoreline that interconnect with critical highways, railways, airports, and pipelines. The Maritime Transportation System (MTS) contributes to one quarter of all United States gross domestic product, or approximately $5.4 trillion.[1] The President has designated cybersecurity of the MTS a top priority for national defense, homeland security, and economic competitiveness.[2]

Maritime Transportation System operators are increasingly using information technology (IT) and operational technology (OT) to maximize the reliability and efficiency of maritime commerce, including: assisting with vessel navigation, communications, shipboard engineering management, cargo management, cargo screening, ballast management, safety, physical security, environmental control, emergency response, and even cargo loading and off-loading.[3] The proliferation of IT across the maritime sector is introducing previously unknown risks, as evidenced by the June 2017 NotPetya cyber-attack, which crippled the global maritime industry for more than a few days.[4] [5] This plan articulates how the United States government can best 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.

The National Maritime Cybersecurity Plan (Plan) for the National Strategy for Maritime Security (NSMS) integrates cybersecurity into the NSMS’s principles of: (1) Freedom of the seas; (2) Facilitation and defense of commerce to ensure the uninterrupted flow of shipping, and (3) Facilitation of the movement of desirable goods and people across our borders, while screening out dangerous people and material.[6]

The Plan unifies maritime cybersecurity resources, stakeholders, and initiatives, aggressively mitigating current and near-term maritime cyberspace threats and vulnerabilities and complements the NSMS’ seven supporting plans.[7] The Plan identifies Federal

[1] United States Committee on the Maritime Transportation System, Why the Maritime Transportation System (MTS) Matters, https://www.cmts.gov/about/why_mts

[2] The White House, National Security Strategy, Washington D.C., 2017, page 13.

[3] (U//FOUO) COVID-19 Losses to Maritime Industry Likely to Prompt Look at More Automation, DHS, May 1, 2020.

[4] Center for Strategic and International Studies (CSIS), Significant Cyber Events since 2006, (Washington D.C.: May 2020).

[5] The Maritime Executive, Naval Dome: Cyberattacks on OT Systems on the Rise, Date of Information: 26-July-2020, accessed 27-July-2020, https://www.maritime-executive.com/article/naval-dome-cyberattacks-on-ot-systems-on-the-rise

[6] The White House, National Strategy for Maritime Security (NSMS), Washington D.C., 2005, Section III.

[7] The White House, National Strategy for Maritime Security (NSMS), Washington D.C., 2005, Annex A. The eight other supporting plans are the National Plan to Achieve Maritime Domain Awareness, Global Maritime Intelligence Integration

government priority actions to close maritime cybersecurity gaps and vulnerabilities over the next 5 years. The Plan's priority actions will evolve as the public sector, private sector, and international partners mature maritime cybersecurity cooperation and initiatives. The National Security Council (NSC) staff, through the NSC policy coordination process, will periodically convene departments and agencies to review progress toward executing the priority actions. Reassessment of this plan will occur at least once every 5 years and it may be revised and/or updated through the policy coordination committee process.

The National Maritime Cybersecurity Plan also supports the 2017 National Security Strategy, the Executive Order (E.O.) on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services (E.O. 13905),[8] the 2018 National Cyber Strategy, and the National Cyber Incident Response Plan; reducing redundancy and maximizing resources to the extent allowable. The Office of Management and Budget will ensure that United States departments and agencies prioritize these efforts in annual budget submissions.

Plan, Maritime Operational Threat Response Plan, International Outreach and Coordination Strategy, Maritime Infrastructure Recovery Plan, Maritime Transportation System Security Plan, Maritime Commerce Security Plan, and the Domestic Outreach Plan.

[8] The White House, Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services, 2020, https://www.whitehouse.gov/presidential-actions/executive-order-strengthening-national-resilience-responsible-use-positioning-navigation-timing-services/

RISKS AND STANDARDS

The MTS subsector is diverse, with businesses of all sizes leveraging IT and OT systems that interconnect with larger maritime systems. Users across the maritime sector access key data and management systems daily for business purposes, making secure access control and user monitoring difficult. Some MTS operators lack the ability to control the security of critical systems because different public and private entities own and operate these interconnected systems. Although cybersecurity standards and frameworks are widely available, businesses often lack the resources or expertise to implement them effectively, leaving them vulnerable to cybersecurity disruptions. Small and medium-sized businesses would benefit from port security or other grant program funding set aside for maritime cybersecurity enhancement projects. Cybersecurity within some ports and facilities is situational, ad-hoc, and often driven by profit margins and efficiency. Unless the private sector has a clear understanding of current and future maritime cybersecurity threats and a financial incentive to invest in maritime cybersecurity measures, some private sector entities may not be inclined to align with maritime partners or Allies.

No single entity owns, controls, manages, or regulates businesses or networks used throughout the maritime domain. MTS stakeholders rely on IT and OT systems to communicate with various transportation nodes to facilitate the movement of goods, illuminating the interdependencies that support our economic prosperity. No one entity standardizes or operates the disparate OT systems within the MTS. Additionally, a large part of the MTS relies on outdated telecommunication infrastructure, threatening the ability for MTS stakeholders to protect digital information, the network, and to detect when malign actors are attempting to access protected systems.

To correct and mitigate these threats, the United States will accomplish the following priority actions.

Priority Actions

Priority Action 1: The United States will de-conflict government roles and responsibilities.

More than 20 Federal government organizations currently have a role in maritime security. These organizations regulate, oversee, and/or manage: vessel and personnel safety, transportation standards, physical security, and other maritime industry roles. Common cybersecurity standards however, do not exist and are not consistent across Maritime Transportation Security Act (MTSA) and non-MTSA regulated facilities. Consistent maritime cybersecurity standards, across maritime industry stakeholders, enable greater coordination to address gaps and vulnerabilities to IT and OT systems allowing exploitation to disrupt maritime commerce. Further, when maritime stakeholders develop common maritime cybersecurity standards, it enables public and private entities to share best practices to mitigate unforeseen cyber vulnerabilities. **The NSC staff, through the policy coordination process, will identify gaps in legal authorities and identify efficiencies to de-conflict roles and responsibilities for MTS cybersecurity standards.**

Priority Action 2: The United States will develop risk modeling to inform maritime cybersecurity standards and best practices.

The United Sates Coast Guard[9] issued reporting guidance to MTSA-regulated facilities and vessel owners and operators regarding security breaches and suspicious activity, including those concerning telecommunications equipment, computers, and network systems. The guidance distributed to MTS stakeholders, however, did not account for cyber incidents that breach a system's defenses or that target administrative systems, unrelated to safe and secure maritime operations. Given the growing number of reports received by the United States Coast Guard regarding maritime cyber events affecting MTSA-regulated facilities, an amendment to the reporting guidance may be necessary to understand the persistence of maritime cyber incidents across MTS owners and operators to help inform new or revised maritime cybersecurity standards. The United States Coast Guard amplified maritime incident reporting guidance, [10] [11] including cyber-related vulnerability information in facility security assessments for MTSA-regulated facilities, however, gaps remain in cybersecurity threshold reporting. [12] **The United States Coast Guard will analyze and clarify the 2016 and 2020 cybersecurity reporting guidance for maritime stakeholders and collect maritime cyber incident reports to identify trends and attack vectors to increase maritime sector situational awareness and decrease maritime cyber risk.**

The National Institute of Standards and Technology (NIST) will construct an internationally accepted, outcome-focused, threat-informed risk framework for port OT systems. Currently, no standard exists for assessing risk in OT networks. An OT risk framework will allow maritime stakeholders, including insurers, facility and/or vessel owners and shippers, to share a common risk language and develop common OT risk metrics for self-assessments. International cooperation, through bilateral engagement or multilateral forums, such as the International Maritime Organization, is critical to align domestic risk standards with international cybersecurity risk standards. Transparency and cooperation will inform a framework, that when used, and will raise adversary costs to compromise maritime systems. **The United States will create an international port OT risk framework based on the input from domestic and international partners and promote the framework internationally**.

Priority Action 3: The United States will strengthen cybersecurity requirements in port services contracts and leasing.

To limit adversarial opportunity, contracts or leases binding the United States Government and private entities must contain specific language addressing cyber risk to the MTS. The private sector owns and operates the majority of port infrastructure. The General Services Administration (GSA) provides minimum Federal government guidelines for Federal contracting. Revised Federal government contracting language is needed to protect Federal departments and agencies from the increased pace of technology proliferation. Port services such as, but not limited to, loading, unloading, stacking, ferrying, or warehousing

[9] United States Coast Guard, Reporting Suspicious Activity and Breaches of Security, 2016.

[10] United States Coast Guard, Reporting, and Investigation of Marine Casualties Where the United States is a Substantially Interested State, 2017.

[11] U.S. Coast Guard, Reporting, and Investigation of Marine Casualties Where the United States is a Substantially Interested State, 2017.12 U.S. Coast Guard, Reporting, and Investigation of Marine Casualties Where the United States is a Substantially Interested State, 2020.

[12] U.S. Coast Guard, Reporting, and Investigation of Marine Casualties Where the United States is a Substantially Interested State, 2020.

Federal cargo requires cybersecurity contracting clauses to safeguard the flow of maritime commerce, MTS users, and our economic prosperity. **United States Federal agencies will work with the GSA to develop and implement mandatory contractual cybersecurity language for maritime critical infrastructure owned, leased, or regulated by the United States government to decrease cybersecurity risk to the Nation.**

Priority Action 4: The United States will develop procedures to identify, prioritize, mitigate, and investigate cybersecurity risks in critical ship and port systems.

The United States will examine critical port OT systems for cyber vulnerabilities. A framework for examining port OT systems does not exist; the maritime sector should glean cyber security best practices from other critical infrastructure sectors that test for cyber vulnerabilities within critical systems. For example, the Department of Energy conducts small-scale vulnerability testing to protect electrical power generation and distribution OT systems. Similarly, maritime OT systems would benefit from vulnerability inspections. Findings from these audits may inform cybersecurity mitigation and remediation for MTS users. Incorporating similar best practices could result in a new framework for maritime cybersecurity specialists to test system vulnerabilities, anonymize applicable information, and share those practices across the maritime sector and international partners.

The Department of Homeland Security (DHS) and the Department of Defense (DOD) will conduct maritime cybersecurity assessments to enhance the protection of port facilities, vessels, and infrastructure from malicious cyber-attacks. Building on existing international frameworks such as the International Ship and Port Facility Security Code provides an opportunity to incorporate a maritime cybersecurity component into foreign port assessments that would not only protect the United States from maritime cyber threats, but also our partners and Allies. **The United States will design a framework for port cybersecurity assessments.**

Partnership with the Federal government is crucial for port owners, shippers, and operators to increase protection and resiliency of IT and OT systems. DHS approves grants to State and local stakeholders to bolster cybersecurity through the Federal Emergency Management Agency (FEMA) Port Security Grant Program. For example, in Fiscal Year 2020, $100,000,000 was available to State and local port stakeholders to enhance port preparedness.[13] **DHS will promote cybersecurity grants and initiatives to protect maritime critical infrastructure.**

The growing dependence on technology demands a maritime cyber-workforce with the capacity and capability to support investigations into major marine casualties and mishaps. Ship and port system vulnerabilities present adversaries with opportunities to masquerade cyber-attacks as accidents. Barring intelligence or law enforcement cueing, these types of incidents could be classified as a traditional major marine casualty or mishap and not attribute the incident to a criminal, or otherwise, nefarious actor(s). Developing and deploying cyber forensics for all major marine casualties and mishaps, when a maritime cyber effect cannot be ruled out, is paramount. **The United States will establish a cyber-forensics process for maritime investigations.**

[13] https://www.fema.gov/grants/preparedness/port-security

Information and Intelligence Sharing

The unique relationships that exist between Federal, state, local, tribal, and territorial governments, industries and industry associations, and other maritime information-sharing organizations present opportunities to address broader cybersecurity vulnerabilities in the MTS. Port owners, operators, and tenants rely on non-standard cybersecurity and information sharing solutions. Information sharing across public, private, and international maritime stakeholders relies on existing partnerships, information sharing agreements, customer needs, and regulatory requirements, all of which bolster maritime cybersecurity defense and resilience. Organizations such as Information Sharing and Analysis Centers provide a pathway to share information across the private and public sector coordinating councils. Transparency, sharing information, and intelligence, as appropriate, are keys to strengthening the integrity and resilience of the MTS.

Priority Actions

Priority Action 1: Exchange United States government information with the maritime industry.

DHS, through the United States Coast Guard and the Cybersecurity and Infrastructure Security Agency (CISA), along with the Federal Bureau of Investigation (FBI) and the intelligence community, will collaborate to develop tear-line reporting and talking points for domestic and international engagement across the maritime sector. Similar efforts exist across other critical infrastructure sectors. **The United States will promote domestic and international engagement to facilitate information sharing and best practices to build a coalition of maritime cybersecurity advocates.**

The Federal government will adapt existing policies and regulations, or create new policies and regulations, that foster the greatest transparency without sacrificing proprietary information to prevent further malicious cyber-attacks. **The United States will establish procedures and policies that govern the receipt and processing of maritime reports of industry cybersecurity incidents to build a coalition of maritime cybersecurity advocates.**

Priority Action 2: Share cybersecurity intelligence with appropriate non-government entities.

The United States will create mechanisms to share unclassified, and when acceptable, classified information with maritime industry stakeholders, increasing access to actionable information to protect maritime IT and OT networks. Credible and actionable intelligence is required to strengthen maritime cybersecurity. Multiple private sector entities claim to be the information-sharing clearinghouse for MTS stakeholders. Overlapping membership across cybersecurity information sharing organizations creates barriers to efficiently inform MTS stakeholders of maritime cybersecurity best practices or threats. For example, CISA and private sector entities have entered into bilateral agreements that allow public and private MTS stakeholders to share information, protecting the proprietary rights of non-public businesses. Through the United States Coast Guard, DHS facilitates processes for sharing information, and potentially, intelligence between MTSA-regulated facilities, private sector partners, and the international maritime community. **DHS will extend domestic successes to identify avenues to share maritime cybersecurity information and intelligence, as applicable, with the international community.**

Priority Action 3: Prioritize maritime cybersecurity intelligence collection.

Because the nation depends on the free flow of maritime commerce, this Plan validates the prioritization of maritime intelligence collection to protect United States interests domestically and abroad. Elevating the importance of maritime cybersecurity in the collection of intelligence requirements provides insights into adversarial tactics, actions, motives, and intent. This enables public and private maritime partners to better prepare and defend networks from adversary exploitation. **The United States will develop and prioritize maritime cyber intelligence requirements, including assessments of partners' cybersecurity needs and capabilities, broadly sharing with MTS stakeholders, to the extent allowable, to guide risk modeling and adversary cyber risk assessments.**

CREATE A MARITIME CYBERSECURITY WORKFORCE

Port OT systems control cargo handling equipment, cranes, scanning equipment, pumps, and cargo inspection services. Vessels use OT systems for propulsion, steering, and ballast management. Malicious actors may use the cyber domain to gain access to these systems to disrupt the flow of maritime commerce causing significant transportation disruptions and regional economic impacts. Cybersecurity is a highly technical field requiring competent cybersecurity specialists to monitor and protect IT and OT systems and assets. The Federal government lacks minimum maritime cybersecurity standards and a commensurate regulatory mechanism to enforce maritime cybersecurity standards across the MTS. As Federal departments and agencies, including the private sector, continue to build their cybersecurity capabilities and workforce talent, minimum training standards need to be identified and baselined to ensure the maximum protection of maritime critical infrastructure. Developing cybersecurity training standards across the maritime sector will close gaps across all components of the MTS.

Priority Actions

Priority Action 1: The United States will produce cybersecurity specialists in port and vessel systems.

Port and vessel systems are unique and not as ubiquitous as commercial office systems. Expertise in port and vessel systems requires time and specialized training. Creating maritime cybersecurity specialists in port and vessel systems requires investment, common training, and a sustainable career path to develop and incentivize cyber professionals. **DHS, through the United States Coast Guard, in coordination with other applicable departments and agencies, will develop cybersecurity career paths, incentives, continuing education requirements, and retention incentives to build a competent maritime cyber workforce.**

Priority Action 2: The United States will collaborate with the private sector to increase maritime cybersecurity expertise.

The interconnectedness between the private and public sectors allows for increased exchanges of best practices and experiences to deepen the skills of a competent maritime cybersecurity workforce. **The Department of Defense and DHS, through the United States Navy and United States Coast Guard will pursue and encourage cybersecurity personnel exchanges with industry and national laboratories, with an approach towards port and vessel cybersecurity research and application.**

Priority Action 3: Develop and deploy a capable maritime cybersecurity workforce.

In 2016, DHS reported the lack of emphasis on cybersecurity training for ports and ships.[14] Federal maritime cybersecurity forces exist, but are not sufficiently staffed, resourced, and trained to monitor, protect, and mitigate cyber threats across the maritime sector. Domestic and foreign ports present risks to vessels, both civilian and military. Ports present the opportunity for adversaries to control commerce and delay force projection. **The United States Coast Guard will field cyber protection teams to support federal maritime security coordination of MTSA-regulated facilities and aid in marine investigations, as required**.

[14] United States Department of Homeland Security, Consequences to Seaport Operations From Malicious Cyber Activity, 2016,pp6

SUMMARY

The United States is a maritime Nation that depends on a robust, integrated, and secure maritime transportation system to support our economic prosperity, provide for our national defense, and connect the United States economy with the global market. Technology innovation develops at a pace faster than that which global maritime security can maintain, creating low-cost opportunities for malicious actors. As critical infrastructure sectors, and their sector specific agencies, anticipate, evolve, and adapt to the increasing interdependencies that technology and automation bring, all levels of government, the private sector, and international partners must continue to collaborate through recognized forums, interagency bodies, and communities to develop, refine, and implement maritime cybersecurity standards, share best practices, and protect the maritime domain that nourishes our economy and protects our national security.

ANNEX A

DIRECTIVES AND STATUTORY PROVISIONS

Presidential Policy Directive (PPD)-18: Maritime Security: Defines the maritime domain as the world's oceans, seas, and waterways. PPD-18 affirms: leveraging public and private sector relationships to enhance maritime domain awareness and sharing relevant information with maritime stakeholders; promoting continuity and resilience of the MTS; facilitating free flow of commerce; and encouraging adoption of security measures in commercial practices. As the introduction of the Internet of Things (IoT) grows within the maritime environment, these themes tie directly into cybersecurity.

PPD-21: Critical Infrastructure Security and Resilience: PPD-21 updates the national approach and calls for improving overall critical infrastructure security and resilience, and specifically cybersecurity. It defines critical infrastructure broadly, including cyber and other systems as well as physical structures across 16 designated United States critical infrastructure sectors led by sector-specific agencies (SSA). PPD-21 promoted the NIST Cybersecurity Framework for use by critical infrastructure owners. The United States Coast Guard and the Department of Transportation are the co-SSA for the Maritime Transportation System Subsector.[15]

PPD-41: United States Cyber Incident Coordination: An increase in the frequency of significant cyber incidents requires synchronizing organizational and government incident response. The private and public sectors have shared interests in safeguarding themselves from malicious cyber activities and in managing cyber incidents and their consequences. PPD-41 outlines the principles, concurrent lines of effort, and leads for the Federal government's national response to significant cyber incidents. The principles include shared responsibility, risk-based response, respecting affected entities, unity of governmental effort, and enabling restoration and recovery. The concurrent lines of effort include threat response, asset response, and intelligence support. Additionally, PPD-41 identifies three ways the Federal government coordinates its activities: national policy coordination, national operational coordination, and field-level coordination. Finally, PPD-41 directs the Secretary of Homeland Security to develop a National Cyber Security Incident Response Plan, in coordination with the Attorney General, the Secretary of Defense, and the heads of other SSAs.[16]

[15] The United States Coast Guard consults with the National Maritime Security Advisory Committee and similar organizations to better understand and address cyber risks in the marine transportation system subsector. At the local level, Federal Maritime Security Coordinators consult with Area Maritime Security Committees (AMSC).

[16] Presidential Policy Directive 41, United States Cyber Incident Coordination (July 26, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident PPD-41 mandated that in coordinating responses to significant cyber incidents, "threat response" activity is led by Department of Justice, acting through the FBI and National Cyber Investigative Joint Task Force; "asset response" activity is led by the Department of Homeland Security, acting through the National Cybersecurity and Communications

E.O. 13636: Improving Critical Infrastructure Cybersecurity (2013): Directs Federal agencies to coordinate with critical infrastructure owners and operators to improve information sharing and to develop and implement risk-based approaches to cybersecurity. Further, it directs the Secretary of Homeland Security to increase cybersecurity information sharing efforts with the private sector, consult on and promote the NIST Cybersecurity Framework, and identify, develop, and maintain a list of critical infrastructure entities where a cybersecurity incident could reasonably result in catastrophic effects to the nation.

E.O. 13691: Promoting Private Sector Cybersecurity Information Sharing (2015): Directs the Secretary of Homeland Security, in coordination with Sector-Specific Agencies and other federal agencies, to strongly encourage the formation of ISAOs. Provides a framework for further sharing of classified and unclassified information with the private sector.

Cybersecurity Information Sharing Act of 2015 (CISA 2015): This act improves cybersecurity throughout the United States by promoting increased information sharing about cybersecurity threats and countermeasures. CISA 2015 requires DHS, in consultation with department and agency partners, to develop the Federal government's capability and process for receiving cyber threat indicators and defensive measures, and directs DHS to share cyber threat information with Federal entities in an automated and real-time manner. CISA 2015 authorizes and encourages private entities to share cyber threat indicators with one another and to monitor their networks for cybersecurity threats, with liability protection, as well as conducting defensive measures.

E.O. 13905: Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing (PNT) Services (2020): Directs Federal departments and agencies to take risk-based approaches to identify responsible use of PNT across critical infrastructure applications, including maritime applications. These approaches include: understanding how the infrastructure relies on PNT; identifying which PNT services are best suited for each application; enhancing the ability to detect disruption and data manipulation of data from PNT services; and enabling infrastructure owners and operators to manage associated risks to their systems, networks, and assets that depend on PNT services.

The Maritime Transportation Security Act (MTSA) of 2002: MTSA addresses port and waterway security and implements International Ship and Port Facility Security Code requirements for the United States. The Act emphasizes the need to protect ports and waterways that are open, exposed, and susceptible to transportation security incidents. MTSA also requires vessels and maritime facilities to conduct vulnerability assessments and develop security plans, and for those assessments to be updated at least every 5 years to account for the changes or evolution of threats and vulnerabilities. Regulations require the owners and operators of MTSA-regulated facilities to analyze vulnerabilities associated with radio and telecommunications equipment, including computer systems and networks. Facility security plans must therefore address cybersecurity vulnerabilities identified in a facility's security assessment. MTSA regulations include the

Integration Center; and intelligence support is led by the Office of the Director of National Intelligence, acting through the Cyber Threat Intelligence Integration Center.

requirement to notify the United States Coast Guard of both breaches of security and suspicious activity, which also include cyber incidents.

Ports and Waterways Safety Act of 1972 (PWSA): Establishes good order and predictability on United States waterways by implementing waterways management practices. The United States Coast Guard has a statutory responsibility to ensure the safety and environmental protection of United States ports and waterways. PWSA authorizes the United States Coast Guard to "establish, operate, and maintain vessel traffic services in ports and waterways subject to congestion”. It also authorizes the United States Coast Guard to require electronic devices necessary for participation in Vessel Traffic Systems (VTS). The combined Ports, Waterways Safety System (PAWSS), and VTS comprise a national system that collects, processes, and disseminates information on the marine operating environment and maritime vessel traffic in major United States ports and waterways.

Security and Accountability for Every (SAFE) Port Act of 2006: Improves maritime and cargo security through enhanced layered defenses. The Act modifies existing legislation, such as the MTSA, and creates and codifies new programs aimed at improving security at United States ports. The Act addresses vessel and facility security plans, including the verification of the effectiveness of such plans through inspections. Identifying cyber threats and vulnerabilities in security plans will continue to be a significant focus in ensuring the safety and security of regulated entities. The Act directs the establishment of interagency operations centers for port security at high-risk ports. The SAFE Port Act of 2006 also authorized FEMA, through the Port Security Grant Program, to provide funding to enhance cybersecurity. Additionally, the SAFE Port Act of 2006 establishes a Port Security Exercise Program to test and evaluate government, commercial seaport personnel, emergency response professionals, the private sector and other stakeholders to prevent, prepare for, mitigate, and respond to emergencies at commercial seaports.

2018 Federal Aviation Administration Reauthorization Act (Division J, section 1805), Cybersecurity Information Sharing and Coordination in Ports: This Act directs the Secretary of Homeland Security, through the United States Coast Guard, to oversee critical infrastructure protection, cybersecurity, and other related DHS programs to: (1) share information related to cybersecurity with State, Federal, local, and private sector stakeholders; (2) develop a Maritime Cybersecurity Risk Assessment Model in accordance with NIST standards; and (3) develop a Maritime Transportation Security Plan to detect, respond to, and recover from cyber incidents.

ANNEX B

OVERVIEW OF THE OPERATIONAL ENVIRONMENT

The Federal government and private industry depend heavily on MTS industries, vessels, infrastructure, logistics networks, and personnel during times of peace, war, and national emergency. Privately owned United States-flagged ships in the inland, coastal, and international trades, United States government-owned military and auxiliary vessels, seafarers, and domestic shipyards and port facilities that support and sustain the maintenance and operations of United States vessels are critical national security resources.[17] United States ships that regularly call foreign ports routinely exchange data with foreign port authorities, port stakeholders, and other port services, including military facilities, over foreign owned and operated networks.

Cyberspace Implications to the MTS

Maritime cyberspace is a global domain consisting of users on interdependent networks of IT infrastructure, OT infrastructure, resident data, the electromagnetic spectrum, and any telecommunications networks, computers, information and communications systems, and embedded processors and controllers related to maritime processes and functions.[18] [19] [20] [21] [22] IT passes and manipulates information for users while OT allows interaction with the physical environment to control machines such as cranes, pumps, and steering systems. The technology ecosystem within the MTS adapts and evolves with faster and more efficient solutions. Public, private, and international MTS stakeholders implement various maritime cybersecurity standards, satisfying domestic, and as appropriate, international standards.

Shipboard IT and OT systems are increasingly cross-connected, requiring internet connections to monitor, update, and input maritime data. The interdependency increases potential risk of unauthorized access and provides additional avenues through which to conduct malicious cyber-attacks to shipboard systems. Additionally, a large part of the MTS relies on outdated telecommunication infrastructure, threatening MTS stakeholders' ability to protect digital

[17] United States Department of Transportation, 2020 Goals and Objectives for a Stronger Maritime Nation: A Report to Congress, February 2020, page 6.

[18] Department of Homeland Security Transportation Security Administration (TSA), 2020 Biennial National Strategy for Transportation Security Report to Congress, David P. Pekoske, 2020, page 35.

[19] Director National Intelligence, Unifying Intelligence Strategy for Maritime, National Intelligence Manager Maritime, March 2020.

[27] Department of Commerce, Special Publication 800-53 revision 4: Security and Privacy Controls for Federal Information

[21] National Security Agency, Committee on National Security Systems Glossary (CNSSI 4009), 06-April-2015, page 40.

[22] Department of Commerce, Special Publication 800-53 revision 4: Security and Privacy Controls for Federal Information Systems and Organizations, National Institute of Standards and Technology (NIST), 22-January-2015.

information and networks, and detect when malign actors are attempting to access protected systems.

Other areas in which cybersecurity affects MTS security and resilience are PNT and satellite communications. Cargo ships around the world drive the global supply chain, all of which rely on PNT services for navigation, offloading cargo, and the operation of on-board cyber systems. For example, the compromise of a vessel's PNT receiver could degrade the ability to navigate safely at sea or within a densely populated waterway, potentially leading to a transportation security incident or maritime accident. To help address these risks within the maritime domain, this Plan advances the responsible use of PNT service per E.O. 13905.[23] Technologies such as Radio Frequency Identification (RFID) and monitoring are effective in locating and identifying cargo; however, these technologies expose the cargo tracking systems to exploitation. DHS, in 2016, predicted that the denial or loss of cargo information could bring port operations to a complete halt if backup was unavailable for cargo information that enables identifying and locating containers, thereby significantly hampering the receipt and distribution of cargo.[24]

Strategic Sealift and Ports: National Defense Considerations

Cyberspace is a warfighting domain in which capable adversaries continually attempt to degrade our Nation's ability to project United States military forces globally. As such, United States Transportation Command (USTRANSCOM) designated "improving mission assurance within the cyber domain" as a top priority.[25] USTRANSCOM is responsible for military power projection, including sealift. Amassing military power projection requires the maritime capability to move large weapons systems and equipment, such as tanks or artillery, as opposed to airlift that may only carry one tank due to size and weight constraints. Moreover, United States Cyber Command has responsibility for protecting Department of Defense information networks, including information networks operating on United States Navy vessels and USTRANSCOM-regulated or operated ships.

In a large-scale military mobilization, the United States' fleet of government-owned surge sealift vessels would provide the majority of strategic sealift capacity. These vessels, maintained around the country in reduced operating status, can be fully crewed and ready for mission assignment within five days of activation. Maintenance of the surge sealift fleet occurs through two separate programs: Military Sealift Command (MSC)'s surge sealift fleet and the Maritime Administration's Ready Reserve Force (RRF).

During an initial mobilization surge, additional deployment and sustaining cargo would be carried by United States-flagged commercial vessels in accordance with the United States Government's

[23] The White House, Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services, 2020, https://www.whitehouse.gov/presidential-actions/executive-order-strengthening-national-resilience-responsible-use-positioning-navigation-timing-services/

[24] United States Department of Homeland Security, Consequences to Seaport Operations From Malicious Cyber Activity, 2016, pp10

[25] United States Transportation Command, Statement of General Stephen Lyons, Commander, United States Transportation Command, Before the Senate Armed Services Committee, February 25, 2020.

"commercial first" policy. Although the United States-flagged commercial fleet is small by global standards, at just under 200 vessels, many American shipping companies have contractual or voluntary relationships with the United States government to provide prioritized access to sealift capabilities.

America's seaports, including more than 70 leading ports, are critical to our Nation's economic and national security.[26] United States military equipment deployed by ship is typically loaded within a strategic seaport. DOD operates six military strategic seaports; additionally, there are 17 designated, commercially-owned and operated ports that voluntarily participate in DOD deployment planning and readiness reporting.[27] [28] [29] There are no designated strategic seaports outside the United States; all planning, outloads, and debarkations at foreign ports occur on a case-by-case basis. The National Port Readiness Network, consisting of military and government agencies, supports military force deployments during national defense emergencies.

The United States military's reliance on the surge fleet for major deployments highlights the need for large-scale, dedicated efforts to improve the cybersecurity posture and resilience of these key resources. Malicious state and non-state actors may target these strategic ports because of their strategic value to the United States and the relative ease of influencing them through cyberspace. For example, more than 90 percent of the military cargo delivered to support Operation Iraqi Freedom was via Military Sealift Command (MSC), the Department of Transportation's Maritime Administration (MARAD), and United States-flagged commercial ships. To put this in perspective, "[f]rom January 2003 through the end of April 2003, MSC delivered more than 21 million square feet of war-fighting equipment and supplies, 260 million gallons of fuel, and 95,000 tons of ammunition to the Persian Gulf area for the Army, Marine Corps, Air Force, and Navy war fighters involved in Operation Iraqi Freedom.[30] Sealift support for military mobilization is critical to defend our national interests.

[26] United States Department of Transportation, Bureau of Transportation Statistics, Port Performance Freight Statistics in 2018, Annual Report to Congress 2019 (Washington, DC: 2020). https://doi.org/10.21949/1504598

[27] Military Ocean Terminal Sunny Point (North Carolina); Joint Base Charleston (South Carolina); Military Ocean Terminal Concord (California); Indian Island (Washington); and Pearl Harbor (Hawaii); and Port Hueneme (California).

[28] Philadelphia (Pennsylvania); Port of Virginia (Virginia); Morehead City and Wilmington (North Carolina); Charleston (South Carolina); Savannah (Georgia); Jacksonville (Florida); Gulfport (Mississippi); Beaumont, Port Arthur, and Corpus Christi. (Texas); San Diego (California); Los Angeles (California); Long Beach (California); Oakland (California); and Anchorage (Alaska).

[29] Surface Deployment and Distribution Command (SDDC) supports the deployment of United States Armed Forces in the event of war, contingency, or other national emergency or disaster. SDDC and other National Port Readiness Network members devote resources to planning for major deployments at these ports and, through various port level committees, specifically Port Readiness Committees established in each of the Strategic Commercial Seaports that are chaired by the cognizant Coast Guard Captain of the Port, builds relationships with local stakeholders in concert with the Maritime Administration's management of the National Port Readiness Network, making ultimate action run smoother than it would otherwise.

[30] Global Security, Sealift in Operation Iraqi Freedom, https://www.globalsecurity.org/military/systems/ship/sealift-oif.htm, retrieved July 21, 2020.

Information Technology and Operations Technology

IT cybersecurity standards and frameworks are widely available, including CISA's Cyber Essentials,[31] the Top 10 Cybersecurity Mitigation Strategies published by the National Security Agency,[32] and the NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity.[33] Although cybersecurity standards and frameworks are widely available, implementation is often challenging, especially for small and medium-sized businesses that may lack the resources or expertise to implement these controls.

Beyond the IT and OT environments directly controlled by the maritime subsector, there are additional vulnerabilities in related systems. Of particular concern are vulnerabilities in electromagnetic spectrum (EMS) technologies, which provide for global connectivity and positioning. EMS systems include satellite signals from the Global Positioning System (GPS), voice communications, and data communications for intra-ship systems, inter-ship systems, and ship-to-shore systems.

Growth of Innovative Technologies

Ports, waterfront facilities, vessels, and Federally regulated waterways leverage automation and data analysis tools to facilitate the throughput and distribution of maritime commerce, goods, and services to domestic and international markets. The expectation is this trend will increase with research, development, and deployment of smart ships and autonomous ships.[34] Over the past 5 years, the MTS has endured malicious cyber activities affecting control systems, security systems such as security cameras and access control technology, navigation systems, and business networks, highlighting that these systems are even more vulnerable. Malicious software can target control systems within critical infrastructure, corrupting processes and potentially deleting or corrupting data.

Some port owners and operators outsource cybersecurity functions while others manage it organically; a situation that further complicates a comprehensive understanding of the network environment and information flow in the MTS. Cybersecurity firms offer differing levels of services and must understand the requirements of the owners and operators along with critical business functions. Additionally, service providers may have foreign ties through investment or other means of influence. Owners and operators must exercise diligence when outsourcing cybersecurity services. Widening the risk, the cybersecurity environment lacks cohesive and practical uniform standards of cybersecurity practices from across the public and private sectors.

[31] https://www.cisa.gov/sites/default/files/publications/19_1106_cisa_CISA_Cyber_Essentials_S508C_0.pdf
[32] https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf?v=1
[33] https://www.nist.gov/cyberframework
[34] Maritime Information Services, China to accelerate smart ship development after CSSC and government agree deal, https://www.porttechnology.org/news/china-to-accelerate-smart-ship-development-after-cssc-and-government-agree-deal/, retrieved July 20, 2020.

Expanded vessel automation emphasizes the need for the integrity of data and availability of digital services. Rapidly increasing numbers of internet-connected devices, known as the IoT, and the rollout of 5G networks will add enhanced connectivity options, which will require strict security, integrity, and confidentiality requirements.[35] Threats from state and non-state adversaries pose a particular threat to supply chains that will require collaboration between private, public, and international stakeholders. Advanced 24/7 cybersecurity technology is critical to monitor and mitigate current and near-term threats rapidly. It is not enough to respond and recover. Cybersecurity technology needs to be able to prevent and remediate intrusions.

Private Sector

ISAC-like organizations have the ability to share best practices amongst partners and peers, but also glean best practices from the public sector, which may contribute to broader community training and education regimes to inculcate a stronger maritime cybersecurity culture.[36] These "for industry, by industry" information sharing centers serve as trusted, well-established, efficient threat information brokers within most other critical infrastructure sectors. Their partnerships with industry stakeholders and with government resources insure timely threat information sharing, anonymized reporting, and critical industry expertise in discussions and responses to cyber and other threats. While ISAC-like organizations do exist within the maritime sector, they do not currently cooperate with each other and have not attained broad industry or government acceptance.

[35] Milo Medin and Gilman Louie, 5G Ecosystem Risks and Opportunities (Washington D.C.: DOD Defense Innovation Board, 03-April 2019).

[36] Currently, United States maritime industry stakeholders are unclear on whether they should share cyber threat information within trusted industry enclaves and when they should report maritime cybersecurity incidents to the United States Coast Guard National Response Center, their local USCG Captain of the Port, CISA's National Cybersecurity and Communications Integration Center (NCCIC), their local FBI field office, and/or the FBI's 24/7 Cyber Watch (CyWatch).

ANNEX C

CURRENT MARITIME CYBER THREATS

This section provides an overview of the current threats from cyberspace and considerations of how cybersecurity affects the maritime domain. This section also examines the actors, motivations, objectives, and proliferation of "gray-zone" operations against critical infrastructure within the maritime subsector including vulnerabilities, risks, gaps, incident reporting, and the assessed future of maritime cybersecurity.

Maritime Cyberspace Actors

The Intelligence Community (IC) assesses that state actors, non-state proxies, and cyber criminals execute cyber campaigns targeting maritime critical infrastructure. In 2019, the Office of the Secretary of Defense designated United States critical infrastructure as a contested space where adversaries have caused, and will continue to cause, damage to United States networks.[37]
As of 2014, nation-state and criminal actors were able to influence the physical environment through cyberspace, including but not limited to OT, Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), distributed control systems (DCS), and programmable logic controllers (PLC).[38]

The cyberspace domain presents an asymmetric opportunity for adversaries to affect our national and economic security without kinetic exchange. The globally interconnected MTS affords adversaries opportunities to conduct maritime cyber-attacks against the United States because execution of these attacks occurs from significant distances to the target(s) and still render considerable economic losses, with variable chances of attribution. As technology develops and proliferates, more state and non-state actors will compete in this domain to gain a competitive advantage. Just as the NotPetya cyber-attack disrupted global commerce, similar malicious activities could follow and directly impact the MTS.

While state-sponsored cyber activities are typically more sophisticated, criminal cyber activities also threaten the United States and occur more frequently with less sophistication. Cybercrime nets approximately $2 trillion annually for cyber criminals and projections indicate an increase to $6 trillion by 2021.[39] [40] Examples of cybercrime activities in the MTS include, among others, ransomware attacks, industrial espionage, and manipulation of data to support smuggling

[37] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
[38] United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-37 Revision 2. Accessed 14-July-2020, https://csrc.nist.gov/glossary/term/operational_technology
[39] Robert Dorey, Managing Ports' Cyber Risk: White Paper, (United Kingdom: British Ports Association and Astaara, June 2020), 11.
[40] U.S Department of Homeland Security, Secure Cyberspace and Critical Infrastructure (Washington D.C: 2020), https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure, accessed 06-July-2020 Robert Dorey, Managing Ports' Cyber Risk: White Paper, (United Kingdom: British Ports Association and Astaara, June 2020), 11.

operations. A 2020 ransomware attack on a shipping company affected protected supply shipments from Australia.[41]

Adversaries frequently interfere with shipboard navigation systems by targeting PNT signals through spoofing or jamming. Spoofing causes intentionally inaccurate ship positioning or time used for critical systems, such as navigation or internet-enabled systems. Jamming prevents reception of positioning and timing data, potentially leading vessels at sea or in a narrow waterway to collide or run aground, hazarding shipping, seafarers, or the marine environment. The majority of these events have occurred against vessels operating in the Eastern Mediterranean Sea, the Middle East, and South East Asia.[42] [43] [44] Fourteen maritime organizations sent a letter to the United States Coast Guard Commandant in 2019 to raise the threat of PNT jamming and spoofing to the IMO Council."[45]

The Office of the Director of National Intelligence (ODNI) assesses the People's Republic of China as a persistent cyber espionage threat to the United States military, economy, and critical infrastructure. China continues to use cyber espionage to strengthen its national and international standing in various sectors, such as transportation, science and technology, military modernization, and economic policy.[46] [47]

The Russian Federation's whole-of-government cyber efforts manifest in malicious cyber-attacks against critical infrastructure sectors including elections infrastructure, energy, and maritime transportation. The 2017 NotPetya malware is a notable and public example of Russian cyberspace operations affecting the maritime environment.[48] [49] This cyber-attack caused in excess of $10 billion in damages and disrupted commercial shipping globally.[50]

Iran presents a multifaceted cyber-espionage, criminal, and cyber-attack threat. Iran sponsors non-State proxies who conduct increasingly sophisticated cyberattacks against critical infrastructure.[51] "Iranian cyber actors [target] United States government officials, government organizations, and

[41] Bruce Sussman, Shipping Giant Hit by 'Nuclear Ransomware' and Vows Not to Pay, https://www.secureworldexpo.com/industry-news/toll-shipping-nuclear-ransomware-attack, retrieved July 20, 2020.

[42] United States Maritime Security Communications with Industry Alerts and Advisories, https://www.maritime.dot.gov/msci-advisories.

[43] The Maritime Executive, Intellectual Capital for Maritime Leaders, Report on Russian Interference, Date of Information: 02-April-2019, accessed 12-April-2020, https://www.maritime-executive.com/editorials/report-russian-gps-spoofing-threatens-safety-of-navigation

[44] United States Department of Homeland Security, Consequences to Seaport Operations From Malicious Cyber Activity, 2016, pp8

[45] The Maritime Executive, Intellectual Capital for Maritime Leaders, Fourteen Maritime Organizations Protest Jamming and Spoofing, Date of Information: 25-June-2019, accessed 01-March-2020, https://www.maritime-executive.com/article/fourteen-maritime-organizations-protest-jamming-and-spoofing

[46] ODNI WW TA 2019 + https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

[47] Brian Fonseca, Chinese and Russian Offensive Cyber Capabilities and Implications to the United States and its Partners in Latin America and the Caribbean, (New America Florida International University: September 2018).

[48] Andy Greenberg, "The untold story of NotPetya: The Most Devastating Cyber-Attack in History," Wired Magazine, 22-August-2018; accessed 22-June-2020, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[49] Brian Fonseca, Chinese and Russian Offensive Cyber Capabilities and Implications to the United States and its Partners in Latin America and the Caribbean, (New America Florida International University: September 2018).

[50] Andy Greenburg, Wired Magazine, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, August 2018.

[51] Intelligence Report: CSIR-17006 Trends in the Targeting of the Maritime Sector, Crowdstrike, May 26, 2017

private sector companies to gain intelligence and position themselves for future cyber operations. Iran continues to set the conditions for cyber-attacks against the United States and its allies. It is capable of causing localized, temporary disruptive effects - such as disrupting a large company's corporate networks for days to weeks similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017."[52] Furthermore, Iran frequently targets OT systems, often the same used in maritime applications. As early as 2012, Iran demonstrated a willingness to target maritime activities by breaching United States Navy unclassified networks.[53]

The Democratic People's Republic of North Korea (DPRK) is a significant cyber threat to companies and institutions with significant financial and material resources. Its goal is largely to generate needed revenue to support its ailing economy. "Pyongyang's cybercrime operations include attempts to steal more than $1.1 billion from financial institutions across the world including a successful cyber heist of an estimated $81 million from the New York Federal Reserve account."[54] [55] The DPRK, however, has demonstrated a willingness and ability to target maritime activities by manipulating multiple RF signals, most notably with South Korea accusing North Korea of spoofing automatic identification systems to evade sanctions.[56] [57]

Attributable or not, the frequency and magnitude of malicious cyber activities affecting the maritime domain and the maritime subsector continues to increase by State and non-State actors. Since 2015, hundreds of small cyber operations compromised of hundreds of gigabytes of maritime-related logistics data and targeted USTRANSCOM subordinate elements. Compromise of this type and size of data provides malicious actors insight into United States strategic mobility plans to deploy military equipment and forces for national defense or foreign humanitarian assistance. In 2018, the United States Navy suffered a breach and theft of significant amounts of data related to United States submarines. The breach revealed Iran's intent of identifying vulnerabilities and gaining technological insight on United States warships.[58] In 2018, the ports of San Diego, California, and Barcelona, Spain, suffered cyber-attacks. The likely objectives of the cyber-attacks were to cause maritime supply chain disruptions to generate economic losses.

[52] Director National Intelligence (DNI), Worldwide Threat Assessment: Statement for the Record of the United States Intelligence Community, Dan Coats, (Washington D.C.: 29-January-2019), 5-9.

[53] FireEye, Operation Saffron Rose, 2013, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf.

[54] Director National Intelligence (DNI), Worldwide Threat Assessment: Statement for the Record of the United States Intelligence Community, Dan Coats, (Washington D.C.: 29-January-2019), 5-9.

[55] Morello and Nakashima, The Washington Post, United States imposes sanctions on North Korean hackers accused in Sony attack, dozens of other incidents, https://webcache.googleusercontent.com/search?q=cache:eSIwe-QuaBEJ:https://www.washingtonpost.com/national-security/us-sanctions-north-korean-hackers-accused-in-sony-attack-dozens-of-other-incidents/2019/09/13/ac6b0070-d633-11e9-9610-fb56c5522e1c_story.html+&cd=2&hl=en&ct=clnk&gl=us, Retrieved July 20, 2020.

[56] FireEye, Operation Saffron Rose, 2013, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf.

[57] NK News, North Korean vessels exploiting tracking system flaws to evade sanctions: report, August 11, 2020, https://www.nknews.org/2019/06/north-korean-vessels-exploiting-tracking-system-flaws-to-evade-sanctions-report/

[58] Center for Strategic and International Studies (CSIS), Significant Cyber Events since 2006, (Washington D.C.: May 2020).

As shown in Table 1, organizations and individuals carrying out these malicious or accidental activities fall into several broad categories with varying motivations and objectives. This list is representational and does not include all categories of groups, motivations, and objectives.

Group	Motivation	Effect
Untrained Employees Hacktivists Disgruntled employees Insider threats	▪ none ▪ reputational damage ▪ disruption of operations	▪ accidental destruction or manipulation of data ▪ intentional destruction of data ▪ publication of sensitive data ▪ media attention ▪ denial of access to the service or system targeted
Criminals	▪ financial gain ▪ commercial espionage ▪ industrial espionage	▪ selling stolen data ▪ ransoming stolen data ▪ ransoming system operability ▪ arranging fraudulent transportation of cargo ▪ gathering intelligence for more sophisticated crimes
Opportunists	▪ the challenge	▪ getting through cyber security defenses ▪ financial gain
States State Sponsored Organizations Terrorists	▪ political gain ▪ espionage ▪ ideology	▪ gaining knowledge ▪ disruption to economies and critical national infrastructure

Table 1: Groups, Motivations, and Objectives[59]

[59] The Guidelines on Cybersecurity Onboard Ships, https://iumi.com/uploads/2018-Cyber_Security_Guidelines.pdf

ANNEX D

TABLE OF ACRONYMS USED

ACRONYM	MEANING
CISA	Cybersecurity and Infrastructure Agency
CISA 2015	Cybersecurity Information Sharing Act of 2015
CSIS	Center for Strategic International Studies
COVID-19	Coronavirus Disease of 2019
DCS	Distributed Control Systems
DHS	Department of Homeland Security
DOD	Department of Defense
EMS	Electromagnetic Spectrum
E.O.	Executive Order
FEMA	Federal Emergency Management Agency
FBI	Federal Bureau of Investigation
GPS	Global Positioning System
IC	Intelligence Community
ICS	Industrial Control Systems
IMO	International Maritime Organization
IoT	Internet of Things
ISAC	Information Sharing and Analysis Center
ISM	International Safety Management
ISPS	International Ship and Port Facility Security
IT	Information Technology
MARAD	Department of Transportation Maritime Administration

MSC	Military Sealift Command
MTS	Marine Transportation System
MTSA	Maritime Transportation Security Act
NIST	National Institute of Standards and Technology
NSC	National Security Council
NSMS	National Strategy for Maritime Security
ODNI	Office of the Director of National Intelligence
OT	Operational Technology
PAWSS	Ports and Waterways Safety System
PLC	Programmable Logic Controller
PNT	Positioning, Navigation, Timing
PPD	Presidential Policy Directive
PRC	People’s Republic of China
PWSA	Ports and Waterways Safety Act
RFID	Radio Frequency Identification
RRF	Ready Reserve Force
SAFE	Security and Accountability for Every Port
SSA	Sector Specific Agency
SCADA	Supervisory Control and Data Acquisition
USTRANSCOM	United States Transportation Command
USCG	United States Coast Guard
VTS	Vessel Traffic System