Emerging Risks in the Marine Transportation System (MTS), 2001-2021

Iris Malone and Anastasia Strouboulis

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC
NCITE NATIONAL COUNTERTERRORISM, INNOVATION, TECHNOLOGY, AND EDUCATION CENTER
A U.S. DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Table of Contents

Abstract: How has maritime security evolved since 2001, and what challenges exist moving forward? This report provides an overview of the current state of maritime security with an emphasis on port security. It examines new risks that have arisen over the last twenty years, the different types of security challenges these risks pose, and how practitioners can better navigate these challenges. Building on interviews with 37 individuals immersed in maritime security protocols, we identify five major challenges in the modern maritime security environment: (1) new domains for exploitation, (2) big data and information processing, (3) attribution challenges, (4) technological innovations, and (5) globalization. We explore how these challenges increase the risk of small-scale, high-probability incidents against an increasingly vulnerable Marine Transportation System (MTS). We conclude by summarizing several measures that can improve resilience-building and mitigate these risks.

About the authors: Iris Malone is an Assistant Professor of Political Science and International Affairs at the Elliott School of International Affairs, George Washington University (irismalone@gwu.edu). Anastasia Strouboulis is a MA Candidate at the Elliott School of International Affairs, George Washington University (astrouboulis@gwmail.gwu.edu)

About NCITE: The National Counterterrorism Innovation, Technology, and Education (NCITE) Center was established in 2020 as the Department of Homeland Security Center of Excellence for counterterrorism and terrorism prevention research. Sponsored by the DHS Science and Technology Office of University Programs, NCITE is the trusted DHS academic consortium comprised of over 60 researchers across 18 universities and non-government organizations. Headquartered at the University of Nebraska at Omaha, NCITE seeks to be the leading U.S. academic partner for counterterrorism research, technology, and workforce development.

Acknowledgement: This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 20STTPC00001-02-01.

Definitions

Advanced Persistent Threats (APTs): a well-equipped adversary that often employs sophisticated methods to stage an attack, typically in the cyber domain

Counterterrorism: practices, tactics, techniques, and strategies designed to prevent, deter, and respond to terrorism

Cyber-attack: the intentional act of attempting to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity

Cyberspace: the interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers

Cyber incident: an incident occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure

Domestic violent extremist: an individual based and operating primarily within the United States or its territories without direction or inspiration from a foreign terrorist group or other foreign power who seeks to further political or social goals wholly or in part through unlawful acts of force or violence

Marine Transportation System (MTS): the global network of land and sea-based infrastructure that facilitates the flow of goods between and within countries; sometimes referred to as the Maritime Transportation System

Maritime Domain Awareness (MDA): effective understanding of information, threats, and anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States

Maritime security: the protection of people and property in the U.S. Maritime Transportation System by preventing, disrupting, and responding to terrorist attacks, sabotage, espionage, or subversive acts

Port security: security, defense, and law enforcement measures employed to safeguard a port and cargo from unlawful or disruptive activities

Risk assessment: product or process evaluating information based on a set of criteria and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making

United States maritime domain: all U.S. ports, inland waterways, harbors, navigable waters, Great Lakes, territorial seas, contiguous zone, customs waters, coastal seas, littoral areas, the U.S. Economic Exclusion Zone and oceanic regions of U.S. national interest, as well as the seas lanes to the United States, U.S. maritime approaches, and the high seas surrounding America

Executive Summary

How has maritime security evolved since 2001, and what challenges exist moving forward? While the Department of Homeland Security (DHS) and U.S. Coast Guard (USCG) implemented several important changes in the wake of September 11 to improve counterterrorism security, these institutions are now challenged by today's complex and expansive threat environment. Identifying these challenges is key to improve Maritime Domain Awareness (MDA) and secure the Marine Transportation System (MTS).

This report provides an overview of the current state of port security, new risks that have arisen since 9/11 and the 2002 Maritime Transportation Security Act, the different types of security challenges these risks pose, and how practitioners may mitigate them. We take a two-pronged research approach to address these questions. First, we conducted a series of interviews with 37 individuals from academia, think tanks, law enforcement, as well as former and active-duty Coast Guard personnel to identify emerging risks. Using these interviews, we then investigated each of these risks in-depth. We used various open-source resources from academic research, think tanks, Government Accountability Office reports, and USCG publications to identify emerging threats and vulnerabilities to the MTS.

Findings: We identify three pressing threats to modern port and vessel security systems:

(1) increasingly diffuse and unorganized set of extremist actors intent on using violence,
(2) increasingly sophisticated cyber-attacks and other Advanced Persistent Threats (APTs), and
(3) advanced technologies and weapons systems.

We also identify a growing number of vulnerabilities in ships, ports, and people whereby these threats can manifest.

Table 1. Summary of Key Vulnerabilities

Vector		Key Vulnerabilities
Ships	Systems	• Operational Technology • Information Technology • Tracking Technology
	Foreign Ports and Routes	• Port Security • Inter-Port Layovers • Natural Chokepoints
	People	• Training • Vetting
	Cargo	• Manifests • Type of Cargo • Shipping Volume
Domestic Port	Ships	• Small Vessel Traffic • Port Congestion • Vessel Size
	Physical Infrastructure	• Physical Security (landlord ports) • Aging Infrastructure • Poor Investment in Maintenance and Modernization • Physical-Cyber Ties
	Digital Infrastructure	• Automated Systems • Networks (Hub and Spoke)

		• Digital Security
People	Companies and Organizational Culture	• Insular Culture • Growing Number of Stakeholders • Governance and Management Challenges • Foreign Operators
	Operators	• Labor Shortages • Unauthorized Access
	Law Enforcement	• Under-Staffing • Slow Resource Acquisition Time • Reverse Machine Learning • Incomplete Information-Sharing

Consequences and Suggested Responses to Emerging Risks: The consequences of these threats and vulnerabilities result in five major challenges practitioners face in navigating an increasingly complex threat environment:

(1) new domains for exploitation,
(2) attribution challenges,
(3) big data and information processing,
(4) technological innovations, and
(5) globalization.

The central challenge to the effectiveness of the laws, regulations, and frameworks implemented in the wake of 9/11 is that the complexity of the current threat environment is outpacing maritime defense and response capabilities. Sophisticated and versatile threats challenge the conventional counterterrorism framework, generating a new set of security challenges. We argue that, unlike the threat environment immediately following 9/11, emerging risks to the MTS are driven by small-scale, high-probability threats. However, interconnected network systems, globalization, and big data create the potential for cascading effects because increasingly interconnected networks of systems make it harder to anticipate exactly how an impact will play out. The nature of the maritime sector—being a "system of systems"—means that an attack in one system has a second-order effect on other, connected systems. This effect can turn a small-scale attack into a major one with little warning.

Based on recommendations and examples introduced in interviews, we identify a series of strategies to improve detection, deterrence, and delivery mechanisms in the MTS. Specifically, our recommendations to leverage these challenges and improve resilience include investments in:

- Machine learning and big data analysis
- Personnel training and operational exercises
- Wargaming and simulation exercises
- Regulations
- Education and lessons learned series

Introduction

How has maritime security changed in the last 20 years, and what risks exist today? Following September 11 (9/11), the sudden, manifest threat of transportation vulnerabilities prompted a paradigm shift within the United States security sector. Within the maritime environment, 9/11 underscored the vulnerability of ports, waterways, and coastal areas to possible terrorist attacks. Al Qaeda was able to meet its primary goal of drawing global attention to its violent jihadist mission overnight. It also provoked concern among U.S. government stakeholders that maritime targets could be similarly attractive to violent non-state actors who aim to gain international publicity by killing civilians, disrupting global commerce, and subverting symbols of the nation's power or interests.

The United States is dependent upon the maritime domain for both trade and security functions. The network of land and sea-based infrastructure that forms the Marine Transportation System (MTS) carries and handles around 80% of all global trade by volume.[1] The United States' MTS is comprised of 25,000 miles of navigable channels, 250 locks, and 3,500 marine terminals.[2] The movement of cargo through the MTS contributes $5.4 trillion in annual commerce—26% of the US GDP—and 31 million jobs.[3]

[1] "Review of Maritime Transport 2018." United Nations Conference on Trade and Development. 2018. https://unctad.org/system/files/official-document/rmt2018_en.pdf

[2] "Maritime Transportation System." U.S. Department of Transportation Maritime Administration. Updated January 8, 2021. https://www.maritime.dot.gov/outreach/maritime-transportation-system-mts/maritime-transportation-system-mts

[3] Schultz, Karl L. "Testimony of Admiral Karl L. Schultz Commandant, U.S. Coast Guard On 'Coast Guard Readiness' Before The House Appropriations Subcommittee On Homeland Security." U.S. Department of Homeland Security. April 28, 2021. p. 3. https://docs.house.gov/meetings/AP/AP15/20210428/112509/HHRG-117-AP15-Wstate-SchultzK-20210428.pdf

In addition to supporting the nation's economic security, the maritime domain is also a crucial element of military mobilization, enabling sealift capabilities and providing logistical support for the deployment of American military forces and materials.[4] Unanticipated disruptions to military deployments could compromise the reliability of the United States' force presence and support to partners. In sum, the MTS is an integral aspect of the United States' global power.

The Homeland Security Act of 2002 organized the Department of Homeland Security (DHS) and its umbrella agencies to mitigate the threat of non-state actors from carrying out terrorist attacks on U.S. soil. As part of this reorganization, the United States Coast Guard (USCG) became responsible for developing effective counterterrorism strategies for the United States' maritime domain. Additionally, Congress and the Department of Homeland Security adopted regulations to respond to international terrorism, including the Maritime Transportation Security Act of 2002 (MTSA) and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act 2006). While these measures substantially improved counterterrorism security in 2002, these institutions are now challenged by today's complex and expansive threat environment.

In order to improve maritime domain awareness, this report traces changes in port security since 2001. Based on a combination of interviews and open-source information, this report identifies several emerging risks to the MTS and port security. We systematically evaluate how these emerging risks to port security may materialize and how Homeland Security Enterprise (HSE) practitioners may leverage big data, machine learning, and training exercises to mitigate these challenges.

Methodology

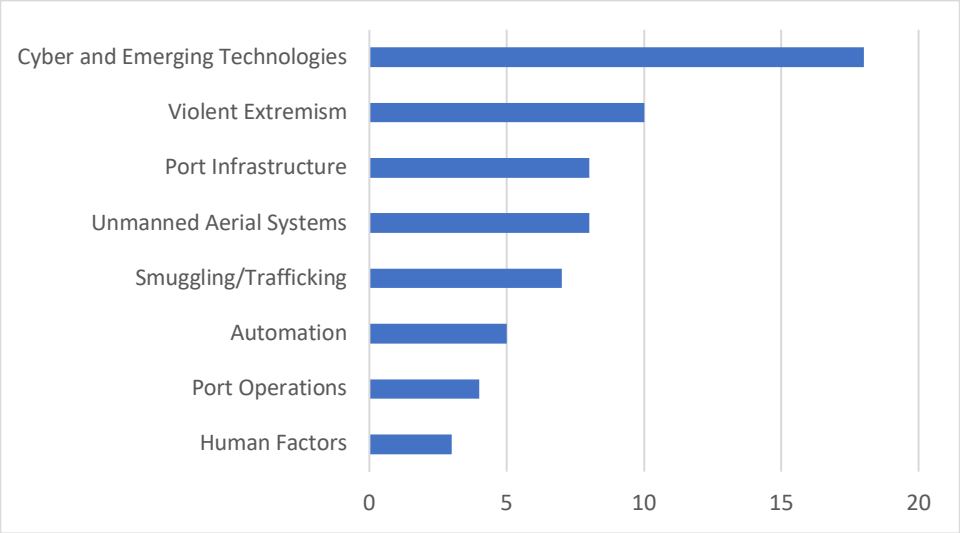
To understand the scale and scope of emerging risks in port security, we undertook a two-pronged research approach. First, we conducted a series of interviews with 37 individuals from academia, think tanks, law enforcement, as well as former and active-duty Coast Guard personnel. Interviewees were asked a systematic set of questions surrounding:

- the current state of port security,
- new risks that have arisen since 9/11 and the 2002 MTSA,
- the different types of security challenges these risks pose,
- and how these challenges may be addressed.

Questions were open-ended in order to solicit the broadest set of answers possible. Despite the professional background diversity of experts interviewed, we found surprising similarities in responses. The most commonly cited risks involved cyber, emerging technology, domestic extremists, port infrastructure, and unmanned aerial systems (Figure 1).

[4] "Maritime Commerce Strategic Outlook." United States Coast Guard. October 2018. https://media.defense.gov/2018/Oct/05/2002049100/-1/-1/1/USCG%20MARITIME%20COMMERCE%20STRATEGIC%20OUTLOOK-RELEASABLE.PDF

Figure 1. Frequency of Emerging Risks Cited in Interviews



Based on the different types of risks enumerated in these interviews, we asked follow-up questions about how and why these risks posed a challenge. We differentiated between two types of risk: threats and vulnerabilities. Threats encompass the new actors, methods, and capabilities that heighten the likelihood of a Transportation Security Incident (TSI). Vulnerabilities encompass the actors, locations, and tools which are susceptible to infiltration, disruption, and interference. This classification scheme helped us discern not only what threats have arisen, but what sectors of the MTS are most vulnerable to specific threats.

Table 1. Categorization of Emerging Threats and Vulnerabilities

Threats	**Vulnerabilities**
Cyber	Port Infrastructure
Advanced Technologies and Weapons	Automation
Violent Extremism	Port Operations
Unmanned Aerial Systems	Opportunities for Smuggling/Trafficking
	Human Factors

Following these interviews, we investigated each of these threats and vulnerabilities in-depth. We used various open-source resources from academic research, think tanks, Government Accountability Office reports, and USCG publications to ground interviewee claims and understand the severity of these risks.

Finally, we organized our findings to create an impact analysis framework. This framework aims to understand what new challenges exist and what policy solutions can mitigate these challenges moving forward. The following sections outline the threats, vulnerabilities, and risk assessments associated with these emerging challenges. We conclude with a series of recommended resilience-building and mitigation strategies that could ameliorate these challenges.

Port Security Since 9/11

Although the September 11 attacks catalyzed massive changes in port security and throughout MTS security, the attacks were not the only TSI at the turn of the 21st Century. We briefly review notable maritime incidents and then explain what measures HSE practitioners took to reduce the risk of these incidents reoccurring.

USS Cole (2000)
On October 12, 2000, the *Cole* was refueling at the port of Aden, Yemen, while on the way to enforce sanctions against Iraq. Two Al Qaeda suicide bombers approached the port side of the guided-missile destroyer in a small, motorized dinghy and detonated the bomb they were transporting.[5] The explosion created a 40-by-60-foot hole in the vessel, killed 17 sailors, and injured 37.[6]

MV Limburg (2002)
The French oil tanker was carrying crude oil from Iran to Malaysia when it approached the port of Mina al-Dabah, Yemen, to pick up another load of oil on October 6, 2002.[7] While it was still nearing the shore, a dinghy loaded with explosives rammed into the starboard side of the tanker and detonated. The vessel caught on fire, and about 90,000 barrels of crude oil leaked into the Gulf of Aden. The explosion killed one person, injured 12, and caused $45 million worth of damage.[8] Al Qaeda claimed responsibility for the attack, and in February 2014, Ahmed al-Darbi pleaded guilty to five charges related to the 2002 bombing of the *Limburg*.[9]

Superferry14 (2004)
The Abu Sayyaf Group (ASG) is a radical Islamist group based in the Philippines, mainly Mindanao. In February 2004, the group bombed the *Superferry14* off the coast of Manila, killing 116 passengers and crew members.[10] Abu Sayyaf was motivated to attack the ferry because the company that owned it, WG&A, did not comply with a letter demanding $1 million in protection money in 2003.[11] This incident is the deadliest terrorist attack at sea to date.

Today, ASG uses the maritime domain for tactical support, including smuggling recruits and goods through the Sulu and Celebes seas.[12] To expand its financial resources, ASG exploits the archipelago of the Philippines to conduct illicit maritime activities, including piracy, drug smuggling, kidnapping for ransom, human trafficking, and arms trafficking.[13] ASG has recently carried out land-based attacks using explosive devices and suicide bombings, indicating its potential reemergence in the maritime domain.

Domestic and International Instruments for Maritime Security

Maritime Transportation Security Act of 2002 (MTSA 2002)

[5] "USS Cole (DDG-67)." Naval History and Heritage Command. October 20, 2020. https://www.history.navy.mil/browse-by-topic/ships/modern-ships/uss-cole.html
[6] Ibid.
[7] "U.S. Charges Saudi for 2002 Oil Tanker Bombing." *The Maritime Executive*. February 6, 2014. https://www.maritime-executive.com/article/US-Charges-Saudi-for-2002-Oil-Tanker-Bombing-2014-02-06
[8] Ibid.
[9] "Guantanamo prisoner al-Darbi admits MV Limburg attack." *BBC News*. February 20, 2014. https://www.bbc.com/news/world-us-canada-26277556
[10] "Superferry14: The World's Deadliest Terrorist Attack at Sea." Safety4Sea. February 27, 2019. https://safety4sea.com/cm-superferry14-the-worlds-deadliest-terrorist-attack-at-sea/
[11] Ibid.
[12] Meghan Curran et al. "Violence At Sea: How Terrorists, Insurgents, and Other Extremists Exploit the Maritime Domain." Stable Seas. p. 151. https://www.stableseas.org/post/violence-at-sea-how-terrorists-insurgents-and-other-extremists-exploit-the-maritime-domain
[13] Ibid, 151.

Immediately following 9/11, the USCG implemented maritime security guidelines that built upon existing knowledge and procedures. However, it soon became clear that a more structured, regulated approach to maritime security was necessary to address the new types of terrorist threats emanating from actors like Al Qaeda. The Coast Guard needed to improve its ability to manage global risks and prevent foreign threats from entering the country. Another motivating factor for the MTSA was to challenge the assumption that all vessels and ports are the same, and therefore measures to protect them should be as well. The MTSA introduced a risk-based methodology to identify security weaknesses and vulnerabilities specific to a facility or vessel. It overall established regulations to reduce the risk and mitigate the exposure of U.S. ports and waterways to terrorist activity.[14]

Congress passed the MTSA in November 2002, and the regulations required by the MTSA were enacted in July 2004. This landmark piece of legislation was "truly the first effort to develop a systematic methodology for maritime security."[15] The goal of the MTSA is to prevent a Transportation Security Incident, defined as any incident that results in significant loss of life, environmental damage, transportation system disruption, and economic disruption to a particular area.[16]

The first foundational component of the MTSA is the facility and vessel vulnerability assessments. The owners and operators are responsible for conducting on-scene surveys and security assessments for their vessels and facilities which are applicable to the MTSA.[17] The vessel and facility assessments identify existing security measures, key vessel or facility operations, potential threats and likelihood of occurrence, and security weaknesses and vulnerabilities.[18]

Another crucial component of the MTSA is the vessel and facility security plans. These security plans include measures to mitigate the vulnerabilities identified during the assessment stage. These measures include passenger, vehicle and baggage screening procedures; security patrols; establishing restricted areas; personnel identification procedures; access control measures; and/or the installation of surveillance equipment."[19] The MTSA also requires the plan to include information on the qualifications and/or training necessary for individuals who have security responsibilities.[20] The Coast Guard performs announced and unannounced inspections annually to determine whether a vessel or facility complies with these MTSA regulations.[21]

The MTSA also mandates designating a Facility Security Officer (FSO) and Vessel Security Officer (VSO). FSOs are responsible for developing, implementing, revising, and maintaining the facility security plan and

[14] "Protecting America's Ports: Maritime Transportation Security Act of 2002." Homeland Security. p. 3. https://www.aapa-ports.org/files/PDFs/mtsa_press_kit.pdf
[15] Steven Hardy. "Maritime Security: A Brief Overview." Homeland Security Digital Library. p. 2. https://www.hsdl.org/?abstract&did=470425
[16] April Tribeck. "Introduction to MTSA: The Maritime Transportation Security Act." United States Coast Guard. p.4. https://www.cisa.gov/sites/default/files/publications/2019-CSSS-USCG-MTSA-101-508.pdf
[17] "33 CFR § 104.305 - Vessel Security Assessment (VSA) requirements." Cornell Law School Legal Information Institute. 2003. https://www.law.cornell.edu/cfr/text/33/104.305
[18] Bill Gasperetti. "Security Since 9/11: Creating the Maritime Transportation Security Act and the ISPS Code." *The Coast Guard Journal of Safety and Security at Sea*. May-December 2017. p. 21. https://www.dco.uscg.mil/Portals/9/DCO%20Documents/Proceedings%20Magazine/Archive/2017/Vol74_No2_May-Dec2017.pdf?ver=2018-01-23-080144-327
[19] "Protecting America's Ports: Maritime Transportation Security Act of 2002." Homeland Security. p. 6. https://www.aapa-ports.org/files/PDFs/mtsa_press_kit.pdf
[20] Bill Gasperetti. "Security Since 9/11: Creating the Maritime Transportation Security Act and the ISPS Code." *The Coast Guard Journal of Safety and Security at Sea*. May-December 2017. p. 22. https://www.dco.uscg.mil/Portals/9/DCO%20Documents/Proceedings%20Magazine/Archive/2017/Vol74_No2_May-Dec2017.pdf?ver=2018-01-23-080144-327
[21] Ibid, p. 22.

liaising with the Coast Guard Captain of the Port and Company and Vessel Security Officers.[22] VSOs are responsible for the vessel's security, including implementing and maintaining the vessel security plan as well as coordinating with FSOs and Company Security Officers.[23]

Area Maritime Security Committees (AMSCs) were also established under the MTSA. There is an AMSC for each of the Coast Guard's 41 Captain of the Port Zones. AMSCs are comprised of at least seven members, each of whom must each have five or more years of experience in maritime or port security operations.[24] Members can be selected from the federal or state government, local public safety and law enforcement personnel, port stakeholders, the maritime industry, or other partners.[25] The purpose of the AMSCs is to "provide a link for contingency planning, development, review, and development of the Area Maritime Security Plans," for their area of responsibility.[26]

Another component of the MTSA is the Transportation Worker Identification Credential (TWIC). The TWIC is an identification credential for all personnel entering unescorted areas of MTSA-regulated facilities and vessels.[27] The TWIC is jointly managed by the Transportation Security Administration (TSA) and the U.S. Coast Guard. TSA is responsible for the enrollment process, while the USCG establishes and enforces access control requirements.[28] TWICs are tamper-resistant, biometrically enabled, and include several overt and covert security features which make them difficult to counterfeit.[29]

Finally, the MTSA mandated the Coast Guard to evaluate the effectiveness of anti-terrorism measures at foreign ports and facilities at least once every three years.[30] This includes evaluating the effectiveness of screening of containerized cargo, security measures to restrict access to only authorized personnel, additional on-board security, licensing, or certification of compliance with security standards, the security management program at the foreign port, and other relevant measures. For ports without effective measures in place, the Coast Guard issues a Port Security Advisory. All vessels arriving to the United States must comply with additional security requirements if it visited ports listed in the Port Security Advisory within the last five ports of call.[31]

Security and Accountability for Every Port Act of 2006 (SAFE Port Act 2006)

As a follow-on to the MTSA, the SAFE Port Act represents another cornerstone of maritime security that focuses on enhancing U.S. port security, preventing threats from reaching the United States, and tracking and

---

[22] April Tribeck. "Introduction to MTSA: The Maritime Transportation Security Act." United States Coast Guard. p. 12. https://www.cisa.gov/sites/default/files/publications/2019-CSSS-USCG-MTSA-101-508.pdf
[23] Ibid, p. 12.
[24] "33 CFR § 103.305 - Composition of an Area Maritime Security (AMS) Committee." Cornell Law School Legal Information Institute. 2003. https://www.law.cornell.edu/cfr/text/33/103.305
[25] Ibid.
[26] "Area Maritime Security Committees." U.S. Department of Homeland Security. p. 2. https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/AMSC%20Brochure%202019.pdf?ver=2019-05-22-080513-100
[27] Ibid, p.16.
[28] Bill Gasperetti. "Security Since 9/11: Creating the Maritime Transportation Security Act and the ISPS Code." *The Coast Guard Journal of Safety and Security at Sea*. May-December 2017. p. 22. https://www.dco.uscg.mil/Portals/9/DCO%20Documents/Proceedings%20Magazine/Archive/2017/Vol74_No2_May-Dec2017.pdf?ver=2018-01-23-080144-327
[29] TWIC Card and Reader Technology. Transportation Security Administration. https://www.tsa.gov/for-industry/twic-card-reader-technology
[30] "46 U.S. Code § 70108 - Foreign port assessment." Cornell Law School Legal Information Institute. https://www.law.cornell.edu/uscode/text/46/70108
[31] "Port Security Advisory (2-20)." International Port Security Program U.S. Coast Guard. December 22, 2020. https://www.dco.uscg.mil/Portals/9/Documents/InternationalPortSecurity/PortSecurityAdvisory/PortSecurityAdvisoryLIBERIARemoveCOE2-20.pdf

protecting containers destined for the United States.[32] The SAFE Port Act created and codified several programs related to maritime security.

The SAFE Port Act established the Container Security Initiative (CSI). The CSI has stationed U.S. Customs and Border Protection (CBP) Officers in foreign locations to inspect containers at foreign ports before placing them on vessels destined for the United States. [33] The CSI aims to identify high-risk containers using automated targeting tools to prescreen and evaluate containers before they are shipped without delaying the movement of commerce.[34]

In addition, the SAFE Port Act provided a statutory framework for the Customs-Trade Partnership Against Terrorism (C-TPAT) program. Through this voluntary public-private partnership, the CBP cooperates with stakeholders within the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers. [35] When stakeholders join C-TPAT, they agree to work with CBP to identify security gaps in the supply chain and implement security measures to mitigate risks. More than 11,400 certified partners in the program have secured benefits from participating in C-TPAT.[36]

International Ship and Port Facility Security (ISPS) Code
The International Maritime Organization (IMO) developed and adopted the ISPS Code in December 2002, which expands upon the principles and regulations on maritime security outlined in the MTSA. It is an amendment to the Safety of Life at Sea (SOLAS) Convention on minimum security arrangements for ships, ports, and government agencies. The measures that the 108 signatories to the SOLAS Convention agreed to came into force in July 2004 and are considered a basis for a "comprehensive mandatory security regime for international shipping."[37] The ISPS Code includes principles on controlling restricted areas, the secure handling of cargo, security procedures and policies, and security training and exercises. The Coast Guard created the International Port Security (IPS) Program in 2004 to align the domestic regulations of the MTSA with the requirements of the ISPS Code.[38]

Current Domestic Capabilities

Consistent with the MTSA, following 9/11, the DHS called for risk-informed approaches to prioritize its investments and develop plans and allocate resources that balance security and global trade.[39] The U.S. Coast Guard created the Maritime Security Risk Analysis Model (MSRAM), a security risk analysis tool used to identify, prioritize, and protect Critical Infrastructure and Key Resources.[40] According to MSRAM, risk = threat

[32] "H.R. 4954: The SAFE Port Act." Committee on Homeland Security. https://www.oas.org/cip/docs/areas_tecnicas/4_proteccion_portuaria/14_the_safe_port.pdf
[33] "CSI: Container Security Initiative." U.S. Customs and Border Patrol. Updated May 31, 2019. https://www.cbp.gov/border-security/ports-entry/cargo-security/csi/csi-brief
[34] Ibid.
[35] "CTPAT: Customs Trade Partnership Against Terrorism." U.S. Customs and Border Protection. Updated May 28, 2021. https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat
[36] Ibid.
[37] "SOLAS XI-2 and the ISPS Code." International Maritime Organization. https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx
[38] Bill Gasperetti. "Security Since 9/11: Creating the Maritime Transportation Security Act and the ISPS Code." *The Coast Guard Journal of Safety and Security at Sea*. May-December 2017. p. 21. https://www.dco.uscg.mil/Portals/9/DCO%20Documents/Proceedings%20Magazine/Archive/2017/Vol74_No2_May-Dec2017.pdf?ver=2018-01-23-080144-327
[39] "Coast Guard: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations." United States Government Accountability Office. December 19, 2011. https://www.gao.gov/products/gao-12-14
[40] Maria G. Burns. "Ensuring Optimum Resilience in Marine Transportation: Extended Applications of the Maritime Security Risk Analysis Model & the Dynamic Risk Management Model." University of Houston College of Technology. June 2014. http://onlinepubs.trb.org/onlinepubs/conferences/2014/MTS2014/Burns.pdf

x vulnerability x consequence. The model calculates risk using threat judgments from the Coast Guard Intelligence Coordination Center (ICC) and vulnerability and consequence judgments from port security specialists at the sector level.[41] MSRAM's risk assessment methodology combines security risks facing different targets with potential attack modes for a target.[42] The model then provides different risk results for each target/attack model combination. This standardized methodology allows for comparing risk levels between targets at the local, regional, and national levels.

The Dynamic Risk Management Model (DRMM) is the risk management tool that uses MSRAM's risk assessment data and methodology to evaluate timelines, investment needs, and priority risks.[43] In combination, DRMM and MSRAM provide risk-based recommendations to inform security decision-making. For example, the MSRAM will state the minimum number of patrols sector commanders must implement, but then they have the discretion to allocate remaining resources based on their local expertise.[44] These tools calculate the relative risk that infrastructures and resources face in their environments to maximize cost-effective resource allocation. There is also a cyber-specific MSRAM in development called the Cyber Risk Assessment Model (MC-RAM). The original MSRAM focuses on the consequences of an attack to develop a cost-effective mitigation recommendation. In a cyber-attack, however, the number of casualties, for example, may not be an input for the consequences variable of the equation. The MC-RAM, therefore, accounts for cyber-specific inputs to mitigate cyber-related risks effectively. In coordination with the AMSCs and relevant Cybersecurity Subcommittees, a series of workshops have been held with stakeholders at port locations throughout the country to define cyber risks for the MTS.[45]

The Marine Transportation System Recovery Unit (MTSRU) is another mechanism within MTS to assist with a disruption. The MTSRU prepares for and conducts recovery operations, mitigates the effects of port closures, and enhances the recovery of MTS operations.[46] The USCG gathers representatives from governmental agencies and the maritime industry to form the MTSRU. The mechanism may be activated when there are "significant delays or interruptions to the continuity of a normally functioning MTS caused by a major event," including a TSI or other natural or human-made disasters.[47] Other stakeholders such as the Captain of the Port, the Incident Command Post, the Port Coordination Team, and the Navigation Restoration Team coordinate with the MTSRU in port recovery activities.

[41] Ibid, p. 11.
[42] Ibid, p. 10.
[43] Maria G. Burns. "Ensuring Optimum Resilience in Marine Transportation: Extended Applications of the Maritime Security Risk Analysis Model & the Dynamic Risk Management Model." University of Houston College of Technology. June 2014. http://onlinepubs.trb.org/onlinepubs/conferences/2014/MTS2014/Burns.pdf
[44] USCG Interview.
[45] "2019 Annual Report." USCG Office of Port and Facility Compliance. p. 10. https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Year%20in%20Review/CG-FAC%20YearInReview%202019_Final.pdf?ver=2020-05-21-081529-687
[46] "Marine Transportation System Recovery Unit." USCG Office of Port & Facility Compliance (CG-FAC) MTSRU. https://homeport.uscg.mil/Lists/Content/Attachments/1626/MTSRU%20Information%20Sheet%20v4%200.pdf
[47] LCDR Navin L. Griffin. "Marine Transportation System Recovery Unit (MTSRU)." Sector Houston-Galveston. May 5, 2017. https://www.lonestarhsc.org/docs/fullcommittee/otherdocs/MTSRU_2017_NLG.pdf

A final area of change has been the digitization and automation of the maritime industry. Over 90% of the global merchant fleet uses digital systems.[48] These systems facilitate communication between ships, crews, and ports; connect with digital navigation and radar systems; support cargo loading, management, and control; replace manual systems for onboard command and control systems; and enhance energy efficiency.[49] In the long term, digitization concepts such as big data, the Internet of Things, and cloud computing will provide new ways to analyze and apply data in real time. Sensors and ship-to-shore communications may also manage semi- or fully- autonomous smart ports and autonomous ships. These developments will likely augment shifts in the design, operation, and monitoring of ship and shore components.

Current Threats Within the Maritime Domain

The events of September 11 exposed the emergent threat of international terrorism and violent jihadism. Many critical infrastructure sites—including major urban areas, port facilities, oil and natural gas platforms, and chemical and nuclear plants—are present along the coast, making them potential targets to outside actors. At the same time, technological innovation has catalyzed the complexity and expansiveness of the maritime system. Adversaries have exploited this environment's inherent and emergent vulnerabilities to create a concurrently more heterogeneous threat landscape. The DHS defines a threat as a "natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property."[50] Interviewees across the maritime industry expressed concern for three threats that persist in this environment: (1) the rise of the cyber domain, (2) the development and deployment of advanced technologies, including unmanned vehicles, and (3) the potential for an international or domestic violent extremist attack. This section of the report discusses the key characteristics of these threats and their applicability to the maritime domain.

The Cyber Domain

In recent years, the maritime industry has leaned into rapid technological development through automation and digitization. The maritime sector has integrated both informational technologies (IT) and operational technologies (OT) to optimize its functioning, comply with legal requirements, and gain a competitive advantage through a forward-thinking business model. Ships and ports have rapidly adapted to the digital environment, including their devices for navigation, communication, sensors, monitoring, cargo, and controllers.

A recent National Security Memorandum on "Improving Cybersecurity for Critical Infrastructure Control Systems" states that "recent high-profile attacks on critical infrastructure around the world…demonstrate that significant cyber vulnerabilities exist across U.S. critical infrastructure."[51] Automation and digitization generated a swath of new risks within the maritime domain; cyber is both an independent threat and a threat multiplier. With the maritime space already vulnerable to inclement weather, natural disasters, smuggling, piracy, and other natural or human-made risk, the potential for a cyber-attack to worsen the impact of these risks, or create new ones entirely, is a pressing concern. The interviews most frequently mentioned cyber

[48] Chalermpong Senarak. "Port cybersecurity and threat: A structural model for prevention and policy development." *The Asian Journal of Shipping and Logistics* 37, no. 1. March 2021. https://doi.org/10.1016/j.ajsl.2020.05.001
[49] Ibid.
[50] "DHS Risk Lexicon." Department of Homeland Security. September 2008. p. 33. https://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf
[51] "FACT SHEET: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure." The White House. July 28, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/

incidents as a top risk. In 2019, cyber incidents were rated second among the top five risks for the maritime and shipping sector.[52]

Tactics. Depending on the attack objective and the target's unique vulnerabilities, a perpetrator can employ a range of cyber-attack tactics both independently and in combination. Several common cyber-attack vectors include:

Table 2. Cyber-attack Vectors

Tactic	Description
Malware	Any malicious software designed to harm or exploit any programmable device, service, or network.
Ransomware	A type of malware that encrypts victims' information and demands payment (usually in Bitcoin) in return for the decryption key.
Phishing	A method of social engineering used to trick people into providing personal or confidential information. Phishing attacks commonly occur via email attachments or links.
Man-in-the-Middle	When a hacker inserts themselves between a device and a server to intercept communications that can then be read and/or altered. Common MITM attacks include IP spoofing, DNS spoofing, HTTPS spoofing, SSL hijacking, email hijacking, Wi-Fi eavesdropping, and stealing browser cookies.
Denial of service (DoS) or distributed denial of service (DDoS)	An attack that attempts to disrupt normal web traffic and take targeted websites offline by flooding systems, servers, or networks with service requests, causing them to crash. A DDoS attack is launched from several host machines that are infected by malicious software controlled by the attacker.

Targets. There are also several potential targets of cyber-attacks within the maritime sector. On land, cargo handling and storage systems and access control systems are vulnerable to attacks. For example, for two years, Dutch-based drug traffickers hired hackers to infiltrate the port of Antwerp's cargo handling system to identify the location of containers from South America where they had hidden cocaine and heroin.[53] Command and control systems, vessel traffic services, and power control systems—including the propulsion and machinery management systems—are all potential targets onboard a vessel. More common, however, are attacks on a ship's numerous navigation systems. For example, the Center for Advanced Defense Studies reported 9,883 instances of Russian Global Navigation Satellite Systems (GNSS) spoofing that affected 1,311 commercial vessels between February 2016 and November 2018.[54] Finally, an attack can target the communication systems, limiting the possibility of a coordinated response on land and at sea, particularly when real-time information cannot be acquired. For example, when the NotPetya virus attacked Maersk, their computer and telephone systems were wiped and inoperable (See Box 1).

[52] "Review of Maritime Transport 2020." UNCTAD. November 2020, p. 119. https://unctad.org/system/files/official-document/rmt2020_en.pdf
[53] Tom Bateman. "Police warning after drug traffickers' cyber-attack." *BBC News.* October 13, 2013. https://www.bbc.com/news/world-europe-24539417
[54] "Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria." C4ADS. March 26, 2019. p. 15. https://c4ads.org/s/Above-Us-Only-Stars.pdf

Box 1. Maersk Global Cyber-attack

In June 2017, A.P. Moller-Maersk (Maersk) was a victim of a cyber-attack caused by the NotPetya malware. As the world's biggest carrier of seaborne freight, in 2017, Maersk was responsible for 76 ports and nearly 800 vessels which transported around 20 percent of the world's global trade by containers.[55] Maersk chairman Jim Hagemann Snabe stated that a Maersk ship carrying 10,000-20,000 containers docks into a port every 15 minutes.[56] Given the scale of Maersk's business operations, the attack on its IT systems affected all eight of its business units, including container shipping, port and tugboat operations, oil and gas production, drilling services, and oil tankers.[57]

The initial infection vector was through a backdoor planted by Russia-based Sandworm hackers in a Ukrainian-based business that used an accounting software called M.E. Doc. By hijacking the company's servers, hackers could release NotPetya to the thousands of other computers globally that had M.E. Doc installed.[58] NotPetya malware leveraged a penetration tool (zero-day exploit) code-named EternalBlue. EternalBlue is a weakness in Microsoft's Windows operating system that allows hackers to remotely run their own programs on an unpatched computer and on other computers within the same network.[59] NotPetya was able to reach patched computers since its creators included a password-stealing tool known as Mimikatz. After gaining initial access to a computer, Mimikatz can pull passwords from a computer's RAM and use them to access other computers with the same credentials.[60] The combination of EternalBlue and Mimikatz allowed NotPetya to spread on its own to rapidly infect connected devices across Ukraine and the globe. Once activated within Maersk's systems, the virus spread within seven minutes.[61] Unlike its predecessor, Petya, NotPetya was not ransomware; payment would not recover lost data.[62] While the cyber-attack target was Ukraine, the collateral damage was global, including the crippling of Maersk's complex global shipping system.

Maersk was forced to shut down all systems across its operations to contain the cyber-attack. Although the computers of individual ships weren't infected, the software on 17 of Maersk's 76 port terminals was disrupted by the attack. In particular, the software which would usually receive the Electronic Data Interchange files from ships—telling terminal operators the contents of their cargo holds—had been entirely wiped.[63] Adam Banks, the former Chief Technology and Information Officer, added that around 3,500 of Maersk's 6,200 servers were destroyed and could not be reinstalled.[64] The attack also undermined a coordinated response because contacts had been wiped from already inoperable

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

[56] Richard Chirgwin. "IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation blitz." *The Register*. January 25, 2018. https://www.theregister.com/2018/01/25/after_notpetya_maersk_replaced_everything/

[57] Sotiria Lagouvardou. "Maritime Cyber Security: concepts, problems and models." Technical University of Denmark. July 5 ,2018. p. 90. https://backend.orbit.dtu.dk/ws/portalfiles/portal/156025857/Lagouvardou_MScThesis_FINAL.pdf

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

[59] Alex Hern. "WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017." *The Guardian*. December 30, 2017. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

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

[61] Rae Ritchie. "Maersk: Springing back from a catastrophic cyber-attack." I – Global Intelligence for Digital Leaders. August 2019. https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack

[62] Alex Hern. "WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017." *The Guardian*. December 30, 2017. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

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

[64] Rae Ritchie. "Maersk: Springing back from a catastrophic cyber-attack." I – Global Intelligence for Digital Leaders. August 2019. https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack

telephones.[65] In sum, NotPetya cost Maersk between $250 million and $300 million.[66] However, Maersk was able to reinstall 4,000 servers and 45,000 PCs, and 2,500 applications within ten days.[67] The company has since made cybersecurity a priority and aims to make its cybersecurity capabilities a "competitive advantage."[68]

Perpetrators. Another new aspect of the cyber threat is the actor or group of actors who aim to exploit cyberspace to achieve their goals. Table 3 summarizes the main actors who are likely to perpetrate cyber-attacks. State actors typically are the most advanced threats, with sophisticated capabilities and resources to carry out multiple, coordinated attacks. However, non-state threat actors have the potential to advance their level of sophistication. For example, during the COVID-19 pandemic, there was a sharp increase in hackers conducting "hands-on" hacking campaigns, which were normally reserved for more skillful nation-state-backed hacking groups.[69]

Table 3. Perpetrators of Cyber-Attacks

Actor	Capability	Motive	Example
State or State-Sponsored	Sophisticated or Significant: Attacks damage or compromise the national security of another nation-state	Soften a target before pursuing conventional military activity; Demonstrate cyber capabilities, hybrid warfare; Undermine economic and cyber power of another nation-state	Russian GPS spoofing in the Black Sea.[70] The attack falsified the location of two NATO warships to be nearby a Russian naval base. If not falsified, this would have been viewed as an act of provocation had the ship truly violated Russian's sovereign waters.
Transnational Criminal Organizations and Pirates	Moderate: Use open-source information or hire cyber-attackers to obtain or modify specific information relevant to group goals	Financial interests, including drug trafficking and piracy operations	Port of Antwerp drug trafficking operations using cargo manifests. Somali pirates targeting vessels traveling through the Gulf of Aden and the Arabian Sea.
Hacktivists and Non-state actors (NSAs)	Unsophisticated or Limited: Attacks disrupt or usurp an organization, but groups have the potential to become more sophisticated.	Ideological motivation to bring awareness to their cause through public attacks; Laying the groundwork for future ransomware attacks.	Hacker affiliated with hacktivist group Anonymous targeted Japanese websites to protest against dolphin hunting.[71] Individual also claimed to hack into the websites of supermarkets and restaurants in Iceland for supplying whale meat.[72] Abu Sayyaf Group (ASG) maritime attacks in the Sulu and Celebes

[65] Ibid.
[66] World Economic Forum. "Securing a Common Future in Cyberspace." January 24, 2018. https://www.youtube.com/watch?v=Tqe3K3D7TnI
[67] Ibid.
[68] Ibid.
[69] Danny Palmer. "Hackers are getting more hands-on with their attacks. That's not a good sign." ZD NET. September 15, 2020. https://www.zdnet.com/article/hackers-are-getting-more-hands-on-with-their-attacks-thats-not-a-good-sign/
[70] H I Sutton. "Positions of Two NATO Ships Were Falsified Near Russian Black Sea Naval Base." *U.S. Naval Institute News.* June 21, 2021. https://news.usni.org/2021/06/21/positions-of-two-nato-ships-were-falsified-near-russian-black-sea-naval-base
[71] Lewis Sanders. "Anonymous hacker downs Japan's tax agency website over dolphin hunting." *DW*. February 10, 2016. https://www.dw.com/en/anonymous-hacker-downs-japans-tax-agency-website-over-dolphin-hunting/a-19037427
[72] Ibid.

			Seas. ASG has typically conducted kidnap for ransom attacks.

Advanced Technologies and Weapons

As automation proliferates throughout the military, so has the development of autonomous weapon systems which select and engage targets with varying degrees of human control. There are three general types of control humans can exercise over an autonomous system, as summarized in Table 4 below.[73]

Table 4. AWS and Human Control

Autonomous Weapons Systems	Degree of Human Control
Semi-autonomous	"Human in the loop"- Human selects target and machine waits for approval from human operator
Supervised autonomous	"Human on the loop"- Machine selects targets, but human operator can intervene and terminate engagements
Fully autonomous	"Human out of the loop"- An activated machine can select and engage targets without intervention by human operator

Perpetrators. In recent years, a non-standard set of actors—terrorist groups, transnational criminal organizations, and other non-state actors (NSAs)—have acquired autonomous weapons systems. Interviewees were particularly concerned with these groups acquiring Lethal Autonomous Weapons Systems (LAWS). While the international community has begun discussing the legal, ethical, and moral questions of LAWS, discussions about limiting autonomous weapons have mainly been limited to state use. NSAs, however, seek these advanced weapons to "level the playing field" against more powerful state forces; LAWS could multiply the impact of an attack during asymmetric warfare. Additionally, the use of LAWS offers a "significant reputational and symbolic benefit" to NSAs, as the ability to acquire and deploy such a weapon "confer[s] a status limited to only a handful of powerful nations."[74] Finally, NSA-operated autonomous weapons would increase the defensive challenges for traditional militaries because their small size and low altitude make them difficult to detect without a more dynamic defense model. [75] Unlike state actors who are subject to international law and domestic regulations, the threat of NSAs acquiring advanced weaponry is concerning since they do not adhere to conventional frameworks of predictability and reliability.

Interviewees expressed concern over two types of autonomous weapons systems: unmanned aircraft systems (UAS), known colloquially as drones, and unmanned surface vehicles (USVs), both of which could be modified to become LAWS.

Several violent NSAs have acquired military-grade UASs from state actors. Iran has exported UASs to groups throughout the Middle East, including Hezbollah, Hamas, and Houthi rebels. Though Iran does not directly deploy UASs, it benefits from the increased proliferation and use of these weapons. These weapons advance Iranian interests by being a force multiplier, an extension of its deterrence capabilities, a method to test weapons and tactics, and a strategy to attack with plausible deniability.[76] In addition to operating its own UASs across

[73] Paul Scharre. "Autonomous Weapons and Operational Risk." Center for a New American Security. February 2016. p. 9. https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Autonomous-weapons-operational-risk.pdf
[74] Philip Chertoff. "Perils of Lethal Autonomous Weapons Systems Proliferation: Preventing Non-State Acquisition." Geneva Centre for Security Policy. *Strategic Security Analysis*, no. 2. October 2018. p. 3. https://dam.gcsp.ch/files/2y10RR5E5mmEpZE4rnkLPZwUleGsxaWXTH3aoibziMaV0JJrWCxFyxXGS
[75] Kerry Chávez and Ori Swed. "Off the Shelf: The Violent Nonstate Actor Drone Threat." *Air and Space Power Journal*. Fall 2020. p. 32. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-3/F-Chavez_Swed.pdf
[76] "Open-Source Analysis of Iran's Missile and UAV Capabilities and Proliferation." The International Institute for Strategic Studies. April 2021. p. 27. https://www.iiss.org/blogs/research-paper/2021/04/iran-missiles-uavs-proliferation

most weight categories, Iran delivers UASs and other advanced weapons through direct transfers, upgrades to existing weapons, the transfer of production capabilities and knowledge, and third-party provision.[77]

When NSAs lack a state sponsor to provide UAS technology and expertise, they tend to acquire and modify commercial UASs to meet their objectives. Hobbyist and commercial UASs are generally affordable; accessible, since regulations are relatively limited; and user-friendly, requiring only some technical or infrastructural knowledge.[78] Still, usually more experienced violent NSAs have the operational maturity to conduct a UAS attack and the strategic capability to manage the consequences of such an attack. For example, between 2016 and 2017, the Islamic State (ISIS) effectively launched 60 to 100 UAS attacks per month by merging "sophisticated commercial off-the-shelf technology with low-tech components and other technological add-ons"[79] (See Box 2). Finally, NSAs may scavenge and reverse-engineer downed military-operated UASs. As evidence, in 2016, IS gathered 18 military-grade UASs, with an Iranian UAS reportedly being used against U.S. forces in 2017.[80]

Non-state actors have also acquired and employed USVs. Remote-controlled vessels, or drone boats, have been used to carry out terrorist attacks, facilitate migrant smuggling, and traffic illicit goods at sea.[81] USVs in shipping lanes pose a significant threat to "the freedom of navigation and commercial shipping interests."[82] For example, in September 2017, an explosive-laden drone boat hit the Saudi Arabian frigate, and in March 2020, four remote-controlled boats were intercepted in an attempted attack on an oil tanker 90 miles southeast of a Yemeni port.[83] In South America, transnational criminal organizations have used low-profile vessels, or self-propelled semi-submersible vessels, to smuggle illicit cargo to Mexico and the United States. Given the success criminal organizations have had in incorporating emerging technology into their operations, they are likely to acquire or invest in "autonomous underwater vehicles to transport narcotics."[84] As one expert on high-tech crime remarked, nascent efforts to construct and deploy remote-controlled vessels illustrate that if autonomous USVs for drug trafficking "don't already exist, they will soon."[85]

[77] Ibid, p. 28.
[78] Ibid, p. 30-31.
[79] Don Rassler. "The Islamic State and Drones: Supply, Scale, and Future Threats." Combating Terrorism Center at West Point. July 2018. p. 4. https://ctc.usma.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf
[80] Ibid, p. 30.
[81] Natalie Klein. "Maritime Autonomous Vehicles within the International Law Framework to Enhance Maritime Security." *International Law Studies*, vol 95. 2019. p. 258. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2907&context=ils
[82] Ibid, p. 261.
[83] H I Sutton. "Disguised Explosive Boat May Be New Threat To Tankers Off Yemen." *Forbes*. March 4, 2020. https://www.forbes.com/sites/hisutton/2020/03/04/new-disguised-explosive-boat-may-threaten-tankers-off-yemen/?sh=267d6d41ad2f
[84] Danielle Muoio. "Here's all the high-tech gear cartels use to sneak drugs into the US." *Business Insider.* July 20, 2016. https://www.businessinsider.com/cartels-use-tech-to-sneak-drugs-into-the-us-2016-7
[85] Ibid.

Box 2. The Islamic State's "Unmanned Aircraft of the Mujahideen" Unit

Between the fall of 2016 and spring of 2017, the Islamic State was at its height of effectively using modified commercial UASs for offensive and defensive purposes. The UAS unit was led by two Bangladeshi brothers who moved funds, UASs, and other dual-use components on behalf of the Islamic State.[86] The group acquired relatively low-cost commercial quadcopter UASs and fixed-wing UAS platforms. These UASs were modified with low-tech add-on components to, for example, drop explosive munitions from above. The Islamic State leveraged its standardized and industrialized weapons manufacturing system and robust supply chain, which consisted of global and layered acquisition channels, to bring its UAS program to scale.[87]

U.S. Special Operations Forces members inspect a drone used by IS to drop explosives on Iraqi forces. Mosul, January 25, 2017. *The Washington Post*

The Islamic States used UASs for various activities, including surveillance and reconnaissance, media productions, command and control for vehicle-borne suicide bombers, and as an attack vector. At its peak in 2017, the Islamic States launched 60 to more than 100 UAS bombing attacks per month across Syria and northern Iraq.[88] Additionally, the Islamic State "treat[ed] UASs as an integral instrument within [its] propaganda machine."[89] Filming and sharing attacks through media channels "highlights the group's claim to effective control of territory and airspace, furthering its claim to 'seeing like a state,' flying like a state, and acting like a sovereign state."[90] Combining mass media with accessible technology supported the group's strategic objective of claiming sovereign statehood.

U.S. forces were largely able to deploy counter-UAS capabilities using expertise from the U.S. Army's Asymmetric Warfare Group.[91] Still, this case study demonstrates how a violent NSA "overcame technical and cost asymmetries and developed a novel weapons system…that challenged the states' ability to respond."[92] Other groups could be inspired to develop their own UAS weapons, tactics, and targets and incorporate them into their hybrid warfare capabilities.

Motives and Tactics. As discussed briefly above, emerging technologies, particularly UASs and USVs, fulfill several objectives. Operational uses include surveillance and reconnaissance, improving command and control, and target acquisition. Actors can also manipulate these emerging technologies to become lethal and perpetrate autonomous attacks. One interviewee distinguished between unmanned vehicles being used for conveyance—such as an offshore vessel carrying WMDs or other lethal goods to a port—and for conducting kinetic attacks. Current military applications of UASs include precision shelling, unmanned airstrikes, and targeted

[86] Don Rassler. "The Islamic State and Drones: Supply, Scale, and Future Threats." Combating Terrorism Center at West Point. July 2018. https://ctc.usma.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf
[87] Ibid, p. 5-6.
[88] Ibid, p. 4.
[89] Emil Archambault and Yannick Veilleux-Lepage. "Drone imagery in Islamic State propaganda: flying like a state." *International Affairs* 96, no. 4. July 2020. https://doi.org/10.1093/ia/iiaa014
[90] Ibid.
[91] T.S. Allen, Kyle Brown, and Jonathan Askonas. "How The Army Out-Innovated The Islamic State's Drones." War on the Rocks. December 21, 2020. https://warontherocks.com/2020/12/how-the-army-out-innovated-the-islamic-states-drones/
[92] Don Rassler. "The Islamic State and Drones: Supply, Scale, and Future Threats." Combating Terrorism Center at West Point. July 2018. https://ctc.usma.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf

assassination and killing. These legitimate uses have also been adopted by malicious actors, for example, in the form of UAS-aided shelling, UAS-guided and led attacks, and loitering munition.[93] Financial objectives include the trafficking of goods or people or, in the case of UASs, creating rogue Access Points (free Wi-Fi networks) to steal user's sensitive information, such as credit card credentials.[94] These emerging technologies are also useful for achieving strategic objectives, including propaganda and deterrence, as demonstrated by the Islamic State and Iran and its regional proxies.

UASs and USVs can reach various targets because they are difficult to detect and can be programmed remotely. These automated technologies could be used for an attack against sea-based infrastructures, passenger ships, fuel tankers, undersea cables and infrastructure, oil and natural gas platforms, and military vessels or infrastructure. For example, an armed Iranian "suicide drone" was recently used to attack an Israeli-linked tanker near the coast of Oman, killing two crew members.[95] Large land-based infrastructure like bridges or dams could withstand a blast from detonating a single UAS's payload. However, UASs or USVs with a larger payload or a coordinated "swarm" attack involving several unmanned vehicles could be more impactful, though conducting a large-scale attack also increases the risk of detection.[96] UAS and drone boats can also target land-based civilian locations, including bridges, ferry or cruise ship terminals, waterfront homes, public areas, and congested cargo unloading stations.

In sum, interviewees viewed automated technologies as a potential threat because of under-developed response and defense capabilities. However, one interviewee expressed that the domestic threat of armed UASs may be deterred by stricter licensing and regulations. This logic supposes that regulations could raise the barriers to deploying UASs in and around ports, although highly-resolved actors may still choose to circumvent these laws. Though these unmanned vehicles may currently be low-impact, as technology advances, these threats will constitute a formidable risk in terms of accessibility, modification, and lowered barriers to reaching ashore.

International and Domestic Violent Non-State Actors (NSAs)

While violent non-state actors tend to target land sites, notable attacks on maritime targets have exposed the vulnerabilities of the MTS. Although the range of actors behind these attacks may differ, they tend to target similar sites using similar weapons and tactics.

Targets. Early incidents of maritime terrorism include the hijacking of the Italian cruise ship *Achille Lauro* by the Palestine Liberation Front (1985), the Al Qaeda attacks on the *USS Cole* (2000) and the French oil tanker *Limburg* (2002), and the explosion on the Filipino *SuperFerry14* (2004), by ASG.

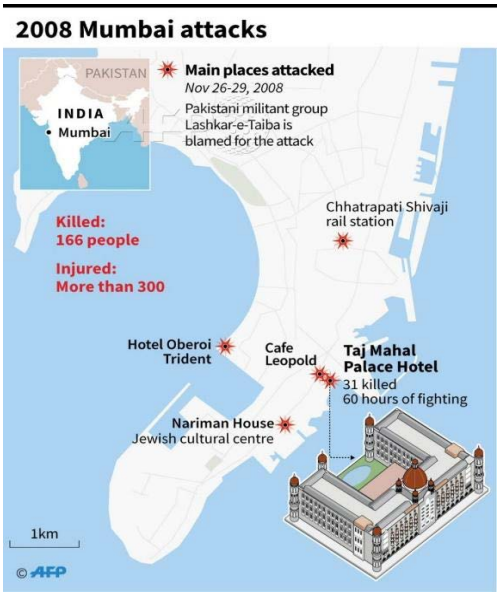
International Violent Extremists. These attacks demonstrate the enduring threat of international violent non-state actors to the MTS due to their global presence and steadfast resolve to undermine the U.S. and U.S.-affiliated targets. Interviewees repeatedly cited the 2008 Mumbai Terrorist attacks to underscore the permeability of maritime borders, and the range of activities violent non-state actors can undertake in such an environment (see Box 3). Leading up to the deadly attacks, Lashkar-e-Tayyiba reconnoitered by sea, trained on Pakistan's inland waterways, departed from the Karachi port, hijacked a fishing vessel, traveled 50 nautical miles, and reached the shores of Mumbai virtually undetected.[97] Hindsight from these maritime incidents

[93] Jean-Paul Yaacoub, Hassan Noura, Ola Salman, and Ali Chehab. "Security analysis of drones systems: Attacks, limitations, and recommendations." *Internet of Things* 11. May 2, 2020. https://dx.doi.org/10.1016%2Fj.iot.2020.100218
[94] Ibid.
[95] Benoit Faucon and Stephen Kalin. "Suspected Drone Attack on Israeli-Linked Tanker in Arabian Sea Kills Two Crew." *The Wall Street Journal.* July 31, 2021. https://www.wsj.com/articles/attack-on-israeli-linked-tanker-in-arabian-sea-kills-two-crew-11627663129
[96] Mauro Lubrano. "Emerging technologies: terrorism and UAVs." Global Risk Insights. January 10, 2018. https://globalriskinsights.com/2018/01/terrorism-uav-risk/
[97] Meghan Curran. "Soft Targets & Black Markets: Terrorist Activities in the Maritime Domain." *Stable Seas.* May 2019, p. 1. https://www.stableseas.org/post/new-report-terrorist-activities-in-the-maritime-domain

illustrates how violent NSAs can exploit the weak and over-stretched security capabilities and infrastructure within the maritime space to pursue political violence.

Box 3. 2008 Mumbai Terrorist Attacks

On November 26, 2008, ten individuals associated with the Pakistan-based extremist group Lashkar-e-Tayyiba (LeT) used a sea route to travel from Karachi, Pakistan, to Mumbai, India. The terrorists hijacked a fishing trawler, killed four crew members, and then docked at the Mumbai waterfront near the Gateway of India monument. They split into three groups and used machine guns and grenades to attack and siege two five-star hotels, the city's largest train station, a Jewish center, a movie theater, and a hospital. From November 26-29, 164 people were killed, plus nine of the attackers. The lone survivor, Mohammed Ajmal Kasab, was executed in November 2012.



AFP News Agency

The sheer size and scale of the maritime environment make identifying potential attack locations challenging. An attack may target U.S. ports, of which there are 361, or those of its 200 foreign trading partners.[98] However, research on maritime attacks from 2010-2017 illustrates that most were concentrated in specific regions of the world: 63 in Sub-Saharan Africa, 27 in Southeast Asia, 21 in Southern Asia, and 15 in the Middle East and North Africa.[99] Additionally, there are well-known shipping chokepoints where a maritime terror attack would be particularly impactful.[100] For example, Safety4Sea identifies the Panama Canal, the Suez Canal, the Strait of Malacca, the Strait of Hormuz, and the Bab el-Mandeb Strait as waterways with structural and geopolitical risks which violent NSAs could capitalize upon.[101]

Domestic Violent Extremists. In addition to international violent NSAs, there is a growing concern for incidents perpetrated by U.S.-based actors, specifically active shooters and domestic violent extremists (DVEs). Recent analysis shows that the current rise in domestic terrorism incidents has been driven by white-supremacist, anti-Muslim, and anti-government extremists.[102] These concerns are echoed by the Intelligence Community and the National Strategy for Countering Domestic Terrorism, which states that "racially or ethnically motivated violent extremists and militia violent extremists present the most lethal DVE threats."[103] In particular, the DHS has highlighted the threat of DVEs targeting government facilities and personnel.[104] The targeting of the USNS

[98] "Targets for Terrorism: Ports." Council on Foreign Relations. 2006. https://www.cfr.org/backgrounder/targets-terrorism-ports
[99] Patricia Schneider. "Recent Trends in Global Maritime Terrorism." In Lucas, Edward R., Thomas Crosbie, Samuel Rivera-Paez, and Felix Jensen (eds.), *Maritime Security: Counter-Terrorism Lessons from Maritime Piracy and Narcotics Interdiction*. NATO Science for Peace and Security Series. 2020. p. 189-190. https://ifsh.de/file/publication/2020-11-26_-Global-Maritime-Terrorism_Schneidery.pdf
[100] See the next section for more on the vulnerability of these chokepoints and other shipping routes.
[101] "Which are the world's most important maritime choke points." Safety4Sea. April 5, 2021. https://safety4sea.com/which-are-the-worlds-most-important-maritime-choke-points/
[102] Robert O'Harrow Jr., Andrew Ba Tran, and Derek Hawkins. "The rise of domestic extremism in America." *The Washington Post.* April 12, 2021. https://www.washingtonpost.com/investigations/interactive/2021/domestic-terrorism-data/
[103] "Domestic Violent Extremism Poses Heightened Threat in 2021." Office of the Director of National Intelligence. March 1, 2021. p. 2. https://int.nyt.com/data/documenttools/biden-administration-domestic-extremist-report-march-2021/ab0bbdf0a8034aea/full.pdf
[104] "National Terrorism Advisory System Bulletin." Department of Homeland Security. May 14, 2021. https://www.dhs.gov/sites/default/files/ntas/alerts/21_0514_ntas_bulletin_all-sectors.pdf

Mercy in March 2020 illustrated how maritime infrastructure and personnel are also considered eligible government targets for new types of domestic extremists (see Box 4). This incident, which was motivated by pandemic-related disinformation, also exemplifies how non-state actors have created and amplified misleading content during the pandemic to manipulate people, incite mistrust in governments, and expand their malignancy activities.[105]

Box 4. Train Targeting USNS *Mercy*

On March 31, 2020, Eduardo Moreno, a train engineer, intentionally ran a train off the tracks in the direction of the USNS *Mercy* hospital ship, which was anchored at the Port of Los Angeles. The train crashed through a series of barriers and fences before halting more than 250 yards from the *Mercy*. Port operations were not seriously affected. Moreno later stated that he was suspicious about the presence of the Navy hospital ship and believed it had an alternate purpose related to COVID-19 or a government takeover. The *Mercy* was there to treat non-coronavirus patients, allowing local hospitals to treat coronavirus patients. On April 2, 2020, Moreno was charged with one count of train wrecking.

Navy Times

Insider Threats. A related concern among interviewees is insider threats, since targeting a port requires knowledge and technical expertise that the general population does not have. An insider threat is defined as the potential for an insider to use their authorized access or understanding of an organization to harm that organization through malicious, complacent, or unintentional acts.[106] An attack could manifest in the form of workplace violence—as demonstrated by the active shooter incidents at Fort Hood and Navy Yard—a cyber-attack, espionage, sabotage, corruption, or theft.[107] Within the maritime sector, there is a potential for a disgruntled employee to "exploit privileged port access to circumvent security safeguards and mount an 'insider' attack."[108] For example, former Navy Reservist Aaron Alexis used his valid credentials as a military contractor to get into the Naval Sea Systems Command headquarters, where he fatally shot 12 people and injured three others.[109] Data reaffirms the risks of potential insider threats to maritime infrastructure, including among those affiliated with the military and law enforcement..[110]

Targets and Tactics. The incidents described above indicate a pattern in the targets, types, and weapons of maritime terrorism. Primary targets include passenger ships, such as the *Superferry14*; oil and gas platforms;[111]

[105] Soraya Binetti, Fabrizio De Rosa, and Mariana Diaz Garcia. "Stop the Virus of Disinformation: the risk of malicious use of social media during COVID-19 and the technology options to fight it." United Nations Interregional Crime and Justice Research Institute (UNICRI). November 2020. http://www.unicri.it/sites/default/files/2020-11/SM%20misuse.pdf

[106] "Defining Insider Threats." Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/defining-insider-threats

[107] Ibid.

[108] Paul W. Parfomak and John Frittelli. "Maritime Security: Potential Terrorist Attacks and Protection Priorities." Congressional Research Service. May 14, 2007. p. 2. https://digital.library.unt.edu/ark:/67531/metadc462262/m1/1/high_res_d/RL33787_2007May14.pdf

[109] Michael D. Shear and Michael S. Schmidt. "Gunman and 12 Victims Killed in Shooting at D.C. Navy Yard." *The New York Times.* September 16, 2013. https://www.nytimes.com/2013/09/17/us/shooting-reported-at-washington-navy-yard.html

[110] Seth G. Jones, Catrina Doxsee, Grace Hwang, and Jared Thompson. "The Military, Police, and the Rise of Terrorism in the United States." April 2021. p. 2. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210412_Jones_Military_Police_Rise_of_Terrorism_United_States_1.pdf

[111] David Blackmon. "Piracy Attacks On Oil Facilities And Vessels: An Issue The U.S. Could Soon Face." *Forbes.* November 20, 2020. https://www.forbes.com/sites/davidblackmon/2020/11/15/piracy-attacks-on-oil-facilities-and-vessels-an-issue-the-us-could-soon-face/?sh=4391764b7734

fuel tankers, as the Houthis have demonstrated;[112] and shipping containers.[113] Other potential targets include military vessels or bases, port industrial plants, and ship channels.[114] In the 2010-2017 period, the most common types of maritime attacks were kidnapping (26 attacks), bombing or explosion (26), hijacking a vehicle (11), and armed assault (10).[115] In this period, only three attacks targeted maritime infrastructure or facilities, illustrating that an attack on this type of target is unlikely to occur physically. In this same period, the most common weapons used were firearms (43) and explosive devices (28).[116] Mines and maritime improvised explosive devices (MIEDS) are "quintessential asymmetric weapons" as they "are cheap, can be easily acquired and deployed; are problematic to counter; are capable of economic disruption; and inflict fear and uncertainty."[117] Other innovations for maritime attack weapons include small boats, including suicide boats and drone boats,[118] diving units with training on deep-sea diving and explosive devices,[119] and fully autonomous vehicle-borne improvised explosive devices.[120]

Since violent NSAs usually aim to gain widespread publicity for their attacks, they are more likely to target highly populated areas or are crucial for the flow of commerce throughout the country. In the United States, hubs of maritime economic activity include the Port of Los Angeles, the Port of Long Beach, the Port of New York and New Jersey, and the Port of Savannah. Given that there is limited precedent for maritime terrorist attacks in U.S. waters and no global shipping chokepoints in North America, external NSA attacks are more likely to target highly-visible domestic locations, or strategic foreign ports and vessels en route to or from the United States.

An important aspect of understanding sea-based violence is that *not all* potential perpetrators of land-based terrorism are also potential perpetrators of maritime terrorism. There is "inherent operational difficulty" in conducting sea and littoral attacks "especially compared to land attacks which may alternatively satisfy terrorist objectives."[121] In addition to the existing security measures taken to harden targets and ensure resiliency, there are tactical challenges and uncertainties that actors would need to overcome to successfully mount a maritime attack. These factors include reconnaissance and surveillance at sea; navigation training; knowledge of tides, currents, winds, visibility, and weather; testing weapons and attack techniques; and ship maintenance and handling. Given this higher barrier to entry, violent NSAs are more likely to develop these sea-based

[112] "Factbox: Attacks, incidents on ships and oil around Saudi Arabia."
[113] Isel Van Zyl and Tyler Lycan. "East African terror groups are exploiting the seas." Institute for Security Studies. October 13, 2020. https://issafrica.org/iss-today/east-african-terror-groups-are-exploiting-the-seas
[114] Paul W. Parfomak and John Frittelli. "Maritime Security: Potential Terrorist Attack and Protection Priorities." Congressional Research Service. Updated May 14, 2007. p. 7. https://digital.library.unt.edu/ark:/67531/metadc462262/m1/1/high_res_d/RL33787_2007May14.pdf
[115] Patricia Schneider. "Recent Trends in Global Maritime Terrorism." In Lucas, Edward R., Thomas Crosbie, Samuel Rivera-Paez, and Felix Jensen (eds.), *Maritime Security: Counter-Terrorism Lessons from Maritime Piracy and Narcotics Interdiction*. NATO Science for Peace and Security Series. 2020. p. 192-193. https://ifsh.de/file/publication/2020-11-26_-Global-Maritime-Terrorism_Schneidery.pdf
[116] Ibid, p. 191.
[117] Peter von Bleichert. "Port Security: The Terrorist Naval Mine/ Underwater Improvised Explosive Device Threat." Walden Dissertations and Doctoral Studies. 2015. p. 8. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=1900&context=dissertations
[118] Abhijit Singh. "Maritime Terrorism in Asia: An Assessment." Observer Research Foundation. October 2019. p. 8. https://www.orfonline.org/wp-content/uploads/2019/10/ORF_OccasionalPaper_215_MaritimeTerrorism-Asia.pdf
[119] Shishir Gupta. "India on alert against possible Lashkar, Jaish attacks from sea." *Hindustan Times.* Updated October 12, 2018. https://www.hindustantimes.com/india-news/india-on-alert-for-terror-attacks-from-sea/story-Z3sbBaWORD4X6R0QZqymaN.html
[120] Kevin S. Knopf. "Fully Autonomous Vehicle-Borne Improvised Explosive Devices—Mitigating Strategies." Naval Postgraduate School. https://www.hsdl.org/?view&did=825210
[121] Paul W. Parfomak and John Frittelli. "Maritime Security: Potential Terrorist Attacks and Protection Priorities." Congressional Research Service. May 14, 2007. p. 23-24. https://digital.library.unt.edu/ark:/67531/metadc462262/m1/1/high_res_d/RL33787_2007May14.pdf

capabilities when maritime access offers strategic utility to the group and when there are not adequate measures to counter these capabilities.[122]

Current Vulnerabilities Within the Maritime Domain

Although the threat environment is becoming more complex, these risks may not necessarily translate into an overt attack. Several legislative measures have improved port security, reduced opportunities for smuggling, and hardened potential maritime targets. However, interviews reveal that changes in the number of actors, systems technologies, and port operations create new maritime vulnerabilities. These generate new opportunities for threats to materialize, jeopardizing the safety and security of ports.

We define vulnerabilities as the collection of physical, cultural, and technological factors that impede maritime domain awareness. These factors can contribute to "sea blindness" or the blind spots which enable adversarial threats to organize, operate, and stage attacks relatively undetected.[123]

Based on interviews with key stakeholders, we identify different vulnerabilities associated with vessels, ports, and humans (Table 5). Globalization, information and communication technologies, port operations, and port infrastructure may amplify the risks.

Table 5. Summary of Key Vulnerabilities

Vector		Key Vulnerabilities
Ships	Systems	• Operational Technology • Information Technology • Tracking Technology
	Foreign Ports and Routes	• Port Security • Inter-Port Layovers • Natural Chokepoints
	People	• Training • Vetting
	Cargo	• Manifests • Type of Cargo • Shipping Volume
Domestic Port	Ships	• Small Vessel Traffic • Port Congestion • Vessel Size
	Physical Infrastructure	• Physical Security (landlord ports) • Aging Infrastructure • Poor Investment in Maintenance and Modernization • Physical-Cyber Ties
	Digital Infrastructure	• Automated Systems • Networks (Hub and Spoke)

[122] Patricia Blacksome and Craig Whiteside. "Rebel Waterways: Modern Militant Use of the Maritime Domain." Maritime Security: Counter-terrorism Lessons from Maritime Privacy and Narcotics Interdiction. Eds. E.R. Lucas et al. IOS Press. August 3, 220. p. 207. https://www.nato.int/cps/en/natohq/topics_181856.htm?selectedLocale=en

[123] Meghan Curran, Christopher Faulkner, Curtis Bell, Tyler Lycan, Michael Van Ginkel, and Jay Benson. Violence At Sea: How Terrorists, Insurgents, and Other Extremists Exploit the Maritime Domain. One Earth Future/Stable Seas Project. August 2020; Dave Mugridge, "Malaise or Farce: The International Failure of Maritime Security," Canadian Naval Review 4, no. 4 (2009): 21.

		• Digital Security
People	Companies and Organizational Culture	• Insular Culture • Growing Number of Stakeholders • Governance and Management Challenges
	Operators	• Foreign Operators • Labor Shortages • Unauthorized Access
	Law Enforcement	• Under-Staffing • Slow Resource Acquisition Time • Reverse Machine Learning • Incomplete Information-Sharing

Ships

Systems

We first examine vulnerabilities related to maritime shipping starting at foreign ports and travel routes. Since 2001, maritime shipping has grown. In order to handle increased traffic, vessels have grown larger, increasing the demand for crew members. Vessel systems have also become more automated to mitigate the risk of accidents due to human error. While these innovations increased the efficiency of maritime shipping, they also create a new swath of vulnerabilities.

Operational and Information Technology Systems. Vessel systems present their own set of vulnerabilities, especially to cyberthreats and human error. Interviews suggested that these automated vessel systems are highly vulnerable to interference and degradation. These vulnerabilities expose vessels to cyber-attacks in several different ways.

OT generally refers to the systems that control engineering, anchoring, and mooring onboard a vessel. There are at least two OT systems vulnerable to cyber interference:

- Mooring and Anchoring: Vessels increasingly incorporate automated mooring to improve the efficiency of docking procedures. A NSA could manipulate the mooring or anchoring systems to direct a vessel to delay operations or run aground.[124]
- Deck and Cargo Machinery: Machinery systems are frequently automated in order to move cargo around a vessel using power winches, cranes, and, in the future, UASs. One concern expressed is that non-state actors could manipulate these systems to smuggle, steal, or move cargo around.[125] For example, a non-state actor could move cargo outside the purview of a security camera in order to manipulate its contents without detection.

There are also aspects of vessel IT systems that are increasingly vulnerable to cyber threats:

- Communication Technology: Industrial radio frequencies for vessel-to-vessel communication are open-source information. However, this standardized protocol means non-state actors can exploit this knowledge to interfere in ship communications. For example, hackers may use low-tech VHF radio systems to impersonate the port authority or block communications between a ship and vessel traffic

[124] Kimberly Tam and Kevin Jones. "Cyber-risk assessment for autonomous ships." In 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp. 1-8. IEEE, 2018.
[125] Ibid.

services.[126] They may direct traffic towards areas where non-state actors can more easily attack a vessel and intercept its cargo. There is also a possibility that non-state actors could exploit communications technology with shore-based control centers to infiltrate port systems and spread malware.[127]

- Sensors: Vessels rely on numerous sensors to obtain information about speed, weather, cargo weight, leaks, and other physical systems. A basic concern is that these sensors could go offline, increasing the risk of a physical incident under poor conditions. Another concern is that an increasingly large number of sensors could lead to "signal congestion" whereby malicious actors exploit a shared operational system to cause these sensors to go down.[128]
- Specialized Navigation Systems (ECDIS, AIS, GPS): These systems are susceptible to jamming and interference by foreign actors. Compromised navigation systems can steer vessels towards hostile waters or cause them to run aground. In 2017, "hackers reportedly took control of the navigation system of a container ship en route from Cyprus to Djibouti for 10 hours."[129] In other cases, these sensors can falsely give vessels the impression of being in the wrong area, raising the risk of an interstate dispute.[130] For example, North Korea allegedly jammed the navigation systems of South Korean fishing vessels between 2010-2016. North Korea then claimed it had the right to use force out of self-defense in order to fend off these nautical intrusions.[131] More recently, the grounding of the oil tanker Wakashio in 2020 may have been due to the manipulation of the digital nautical display chart ECDIS system by unknown actors.[132]
- Security and Monitoring: Closed Circuit Television Camera (CCTV) and other onboard security monitoring systems are vulnerable to interference by crew members who might have unchecked access.[133] The concern is that unvetted crew (see more below) could manipulate these systems to reduce visibility in key areas.

Tracking Technology. In addition to OT and IT systems, tracking systems are also increasingly vulnerable to cyberthreats, piracy, and physical attacks. AIS systems can increase a ship's vulnerability to a range of attacks by NSA because they provide an over-abundance of real-time targeting information. Public and easily accessible information makes reconnaissance easier for attack planning.

For example, the public website *MarineTraffic* uses AIS information to publicly track large vessels around the world.[134] This information allows companies to view when and where shipments are expected to arrive. However, it also gives NSAs valuable details on where to intercept and interdict vessels. For example, Somali pirates have allegedly used public information from websites like these to intercept vessels en route.[135] Open-source tracking systems can increase vulnerability to more lethal attacks as well. For example, international

[126] Jeremy Wagstaff. "Global shipping fleet exposed to hacking threat." Reuters. 2014. https://www.reuters.com/article/us-cybersecurity-shipping/all-at-sea-global-shipping-fleet-exposed-to-hacking-threat-idUSBREA3M20820140424
[127] Kimberly Tam and Kevin Jones. "Cyber-risk assessment for autonomous ships." In 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp. 1-8. IEEE, 2018.
[128] Ibid.
[129] Fred S. Roberts, Dennis Egan, Christie Nelson, and Ryan Whytlaw. "Combined Cyber and Physical Attacks on the Maritime Transportation System." Command, Control, and Interoperability Center for Advanced Data Analysis. DHS Center of Excellence. 2019. https://par.nsf.gov/servlets/purl/10166239
[130] Jonathan Saul. "Cyber threats prompt return of radio for ship navigation." Reuters. 2017. https://www.reuters.com/article/us-shipping-gps-cyber/cyber-threats-prompt-return-of-radio-for-ship-navigation-idUSKBN1AN0HT
[131] "North Korea jamming signals near South border." BBC. 2016. https://www.bbc.com/news/world-asia-35940542
[132] Nisha Degnarain. "Could Oil Ship Wakashio Been Hacked Before Mauritius Spill?" Forbes Magazine. 2020. https://www.forbes.com/sites/nishandegnarain/2020/10/26/could-mol-chartered-mauritius-oil-spill-ship-wakashio-have-been-hacked/?sh=2f3858d77fbb
[133] Kimberly Tam and Kevin Jones. "Situational Awareness: Examining Factors that Affect Cyber-Risks in the Maritime Sector." *International Journal on Cyber Situational Awareness* 4 (2020). 10.22619/IJCSA.2019.100125.
[134] See https://www.marinetraffic.com/
[135] Jeremy Wagstaff. "Global shipping fleet exposed to hacking threat." Reuters. 2014. https://www.reuters.com/article/us-cybersecurity-shipping/all-at-sea-global-shipping-fleet-exposed-to-hacking-threat-idUSBREA3M20820140424

terrorist groups have previously used Google Earth to scout security around military targets and oil facilities (Box 5).[136]

Box 5. Google Earth and Terrorist Attacks

In 2005, Google released its "Google Earth" tool, which provided high-resolution satellite imagery of sites around the world for public usage. Soon after, jihadist forums began discussing the possibility of using Google Earth in lieu of conventional physical reconnaissance. In July 2006, the Islamic Army of Iraq used Google Earth for tactical reconnaissance of US military sites around Rasheed Airport in Iraq.[137]Authorities discovered the tool when a jihadist posted an online video to a website. One of the screenshots from the 19-minute video featured a browser tab of Google Earth.

Screenshot from video of Google Earth demonstration. Arabic language captions translate as "Islamic Army in Iraq/ The Military Engineering Unit--Preparations for Rocket Attack."

Open Source Center Report (2006)

Beyond container shipping, open-source tracking information poses a particular risk for ferries and cruise ships. Ferries, cruise ships, and other passenger vessels often travel along predefined routes according to established locations and departure and arrival times.[138] These schedules are "both fixed and highly transparent, availing terrorists with a reasonably accurate cartographic picture that can be used to gauge the point at which vessels are most susceptible to attack and interception."[139]

Foreign Ports and Routes

Due to increased shipping traffic, vessels now make more inter-transport stops and rely more heavily on chokepoint routes. Foreign port stops and routing decisions increase opportunities for NSAs to disrupt or interfere with container shipping cargo.

Verification Regimes at Foreign Ports. Numerous safe protections have been undertaken to bolster port security under the authority of the MTSA, SAFE Porrt Acts, and Coast Guard Office of International and Domestic Port Security. However, gaps in port security remain. One limitation cited in interviews is the voluntary nature of the C-TPAT program. Since participation in C-TPAT is voluntary, there is a concern that there remain stakeholders

[136] "The Google Controversy – Two Years Later." Open Source Center. 2008. https://fas.org/irp/dni/osc/google.pdf
[137] "Iraqi Insurgency Group Utilizes Google Earth for Attack Planning." Open Source Center Report July 2006. https://fas.org/irp/dni/osc/osc071906.pdf
[138] Michael D. Greenberg et al. "Maritime Terrorism: Risk and Liability." RAND Corporation. 2006. p. 97. https://www.rand.org/content/dam/rand/pubs/monographs/2006/RAND_MG520.pdf
[139] Ibid, p. 97.

in at-risk ports who do not conform to these standards.[140] Weak verification regimes can facilitate smuggling, trafficking, and poor information-sharing between foreign and domestic port operators. This can raise the risk of illicit goods entering the United States. However, interviews suggested this risk has greatly diminished over the last 20 years. While present, it is not as pressing as some other vulnerabilities cited in this report.

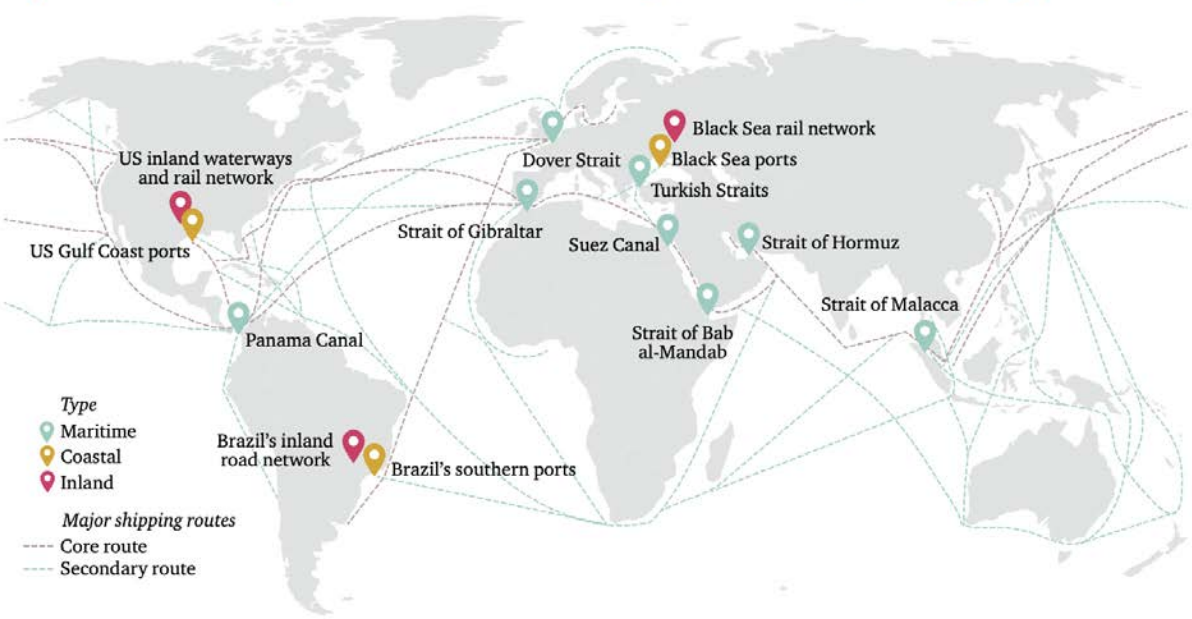
In addition to inconsistent verification regimes, there are also concerns about relative corruption and transparency at foreign ports. Corruption at foreign ports may make it easier to manipulate cargo contents. For example, the U.S. Agency for International Development canceled its support for the Port of Odessa in Ukraine due to corruption and the port organizations' resistance to requested reforms.[141] There are similar concerns that corrupt customs officers in foreign ports may permit organized smuggling to occur in exchange for bribes. Corruption can also result in the mismanagement of funds. If funds to bolster port security are siphoned to particular stakeholders, then ports may remain vulnerable to attacks despite ostensible investments.

Inter-Port Layovers. In order to improve shipping efficiency, vessels now make more frequent stops between their port of origin and port of arrival. This allows shipping companies to maximize cargo loadings on short-haul trips and reduce transportation costs. However, more frequent stops also increase the number of opportunities for tampering with cargo. For example, Flynn (2006) outlines a scenario where a container could leave a C-TPAT certified port, but stop in a non-certified port as a layover. There, a violent NSA could remove the seal, add a weapon into the container, and replace the seal with a forgery. Because CBP typically evaluates container shipping risk based on port of origin and port of arrival, the container would be deemed low risk upon its arrival in the United States.[142] These practices increase the likelihood of human trafficking or illicit cargo entering the country.

Natural Chokepoints. The increase in container shipping traffic means vessels today rely more heavily on a number of designated shipping routes. These shipping routes often traverse natural chokepoints, a narrow international waterway where interdiction is possible by state or non-state actors.[143] Maritime traffic frequents through eight well-known chokepoints: Panama Canal, Strait of Gibraltar, Dover Strait, Turkish Straits, Suez Canal, Strait of Bab al-Mandab, Strait of Hormuz, and Strait of Malacca. As vessel traffic increases, there is a growing dependency on these different chokepoints. "A smaller but nonetheless significant share [of agricultural exports] – 10 percent – now depends on transit through one or more of the maritime chokepoints as the only viable shipping route, up from 6 percent in 2000."[144] Approximately 30% of all maritime crude oil goes through the Strait of Hormuz.[145] There are two types of vulnerabilities associated with these shipping routes.

[140] Aaron C. Davenport. "Lessons from Maritime Narcotics Interdiction: Interdiction in the Maritime Source, Transit, and Arrival Zones of the Western Hemisphere." Maritime Security: Counter-Terrorism Lessons from Maritime Piracy and Narcotics Interdiction 150 (2020): 3.
[141] "US Ends Aid for Port of Odessa Customs Reforms." Maritime Executive. 2016. https://www.maritime-executive.com/article/usaid-ends-aid-for-port-of-odessa-customs-reforms
[142] Flynn, Stephen E. "Port security is still a house of cards." Far Eastern Economic Review 169, no. 1 (2006): 5-11.
[143] Alexander, Lewis M. "The Role of Choke Points in the Ocean Context." *GeoJournal* 26, no. 4 (1992): 503-09. Accessed July 21, 2021. http://www.jstor.org/stable/41145437.
[144] Rob Bailey and Laura Welles. "Chokepoint Vulnerabilities in Global Food Trade." Chatham House. 2017. https://www.chathamhouse.org/sites/default/files/publications/research/2017-06-27-chokepoints-vulnerabilities-global-food-trade-bailey-wellesley-final.pdf
[145] World Oil Transit Chokepoints Analysis Brief. US Energy Information Administration. 2019. https://www.eia.gov/international/analysis/special-topics/World_Oil_Transit_Chokepoints

Figure 2. Natural Chokepoints in Maritime Shipping Routes



Source: Shipping routes adapted from Rodrigue, J.-P., Comtois, C. and Slack, B. (2017), *The Geography of Transport Systems*, New York: Routledge, https://people.hofstra.edu/geotrans/.

First, there is a concern that traffic is over-dependent on access to and safe passage through these chokepoints. If these chokepoints become inaccessible, delays in transportation would have severe economic costs. They would not only cost shipping companies in re-routing and delayed shipping times, but it could disrupt global supply chains.

Some chokepoints are associated with few alternative shipping routes should something happen. For example, the Turkish Straits is perceived as an increasingly vulnerable part of the MTS due to increased grain exports moving from the Black Sea region.[146] There is a fear that interstate tensions could cause Turkey to nationalize the ports to restrict access, or that the terrorist Islamic State could try to stage attacks on the Straits.[147] Given the increasingly interconnected MTS, these delays could have cascading effects that harm the global economy.

[146] Polina Devitt. "Black Sea wheat exports seen steady in 2020/21: Reuters poll." Reuters. June 11, 2020. https://www.reuters.com/article/us-blacksea-wheat-poll/black-sea-wheat-exports-seen-steady-in-2020-21-reuters-poll-idUSKBN23I2BP

[147] Rob Bailey and Laura Welles. "Chokepoint Vulnerabilities in Global Food Trade." Chatham House. 2017. https://www.chathamhouse.org/sites/default/files/publications/research/2017-06-27-chokepoints-vulnerabilities-global-food-trade-bailey-wellesley-final.pdf

Box 6. Ever Given and the Suez Canal

In March 2021, the mega-size container ship Ever Given grounded in the Suez Canal while traveling en route from Tanjung Pelepas to Rotterdam. The consequences of this grounding rippled throughout the global supply chain; approximately 12% of global trade passes through the canal every day. The incident occurred when strong winds shifted the direction of the ship, which caused it to run aground. The ship caused massive congestion and backlog on the Suez Canal. Estimates suggest the grounding blocked $9.6 billion in trade from traveling through the Suez Canal. Some ships were forced to undergo costly rerouting around the Cape of Good Hope, adding eight days to their journey. Approximately 369 ships that had already entered the Suez Canal found themselves stranded behind the Ever Given. The container ship remained stuck for five days as local dredgers and tugboats attempted to free the ship to continue on the journey.[148]

Maxar Technologies/AP

Second, there is a concern that ships traveling through these chokepoints are at increased risk of a targeted attack. Some chokepoints are more vulnerable to attacks than others due to their geopolitical significance, proximity to weak states, lack of alternative routes, and inadequate international cooperation on building resilience. If a chokepoint closed, state or non-state actors could target vessels to intimidate and coerce adversaries. For example, during the Tanker War, Iran and Iraq routinely targeted oil tankers carrying supplies through the Strait of Hormuz.[149]

Vessels traveling through chokepoints are also vulnerable to infiltration or targeted violence due to their exposed nature. More recently, the Houthis in Yemen have exploited the Bab el-Mandab strait to attack Saudi oil tankers, forcing the suspension of travel.[150] NSAs could also leverage their knowledge about alternative routes to target and intercept diverted traffic.

People

A final set of vulnerabilities associated with ships concern the potential for human interference and error. These are most likely to manifest due to poor crew training and crew vetting.

[148] Mary-Ann Russon. "The cost of the Suez Canal blockage." BBC. 2021. https://www.bbc.com/news/business-56559073

[149] "Strait of Hormuz: Assessing the threat to oil flows through the Strait." Strauss Center. N.d. https://www.strausscenter.org/strait-of-hormuz-tanker-war/

[150] Rania el Gamal. "Saudi Arabia halts oil exports in Red Sea lane after Houthi attacks." Reuters. 2018. https://www.reuters.com/article/us-yemen-security/saudi-arabia-halts-oil-exports-in-red-sea-lane-after-houthi-attacks-idUSKBN1KF0XN

Crew Training. Crew error due to poor training standards can increase a vessel's vulnerability to both physical and cyber threats. In a survey conducted by the University of Plymouth Maritime Cyber Threats research group, "74% of participants ranked crew-training standards as the top problem" in maritime security.[151] An added concern is a lack of awareness, training, and expertise on basic cybersecurity requirements and cyberthreat management, particularly as it relates to maritime operations and infrastructure.[152] This "human factor" creates opportunities for cyber threats to permeate the network of a ship and infect critical infrastructure. For example, as crew members bring an increasingly large number of personal devices onboard, namely smartphones and USB drives, there is a concern that they could spread malware by connecting their devices into the vessel mainframe.[153] In other cases, a crew member may unintentionally expose the vessel to a cyber-attack. A crew member could infect a ship's computer systems with malware by inserting a compromised USB drive into vessel computing systems. When this happened in 2017, a second crew member inadvertently magnified the scale of the threat by allowing the malware to infect the navigation systems when he went to update the computer.[154]

The COVID-19 pandemic exacerbates this risk. Vessels are understaffed due to crew shortages caused by the pandemic. [155] Travel restrictions and virus controls make it harder to replace crew, increasing the risk of a fatigued or exhausted crew onboard. Exhaustion can make crew members susceptible to simple mistakes—such as opening a suspicious email—or more dangerous ones—such as a lack of situational awareness—which can result in a TSI.[156] Some interviews also expressed concern about the consequences of the COVID-19 pandemic on crew and port operator health. Existing research already identifies a growing set of physical and mental health challenges which may make crew vulnerable to blackmail, "sextortion," phishing attempts, or deliberately perpetrating an attack.[157]

Crew Vetting. A second factor that can magnify the risk of human error onboard ships is poor crew vetting. The majority of vessels that disembark in the United States have foreign crews.[158] Since foreign crews are hired overseas, there is a possibility of poor vetting. Approximately one-quarter of crew members come from the Philippines and move 90% of global trade. Crew members also come from China, Vietnam, India, and Myanmar.[159] These countries differ in their training and recruiting processes which result in varying security risks. In some cases, crew may intentionally attempt to smuggle goods. In 2020, US Customs and Border Patrol reported a crew member who was found to be loading bulk cocaine onto speedboats from a vessel.[160] The cruise

[151] Kimberly Tam and Jones, Kevin. "Situational Awareness: Examining Factors that Affect Cyber-Risks in the Maritime Sector." International Journal on Cyber Situational Awareness, 4 (2020). 10.22619/IJCSA.2019.100125.
[152] Juan Ignacio Alcaidea and Ruth Garcia Llave. "Critical infrastructures cybersecurity and the maritime sector." *Transportation Research Procedia* 45. March 20, 2020. https://doi.org/10.1016/j.trpro.2020.03.058
[153] Chris Baraniuk. "How Hackers are targeting the shipping industry." BBC. 2017. https://www.bbc.com/news/technology-40685821
[154] Ibid.
[155] Costas Paris. "Ships are moving, but exhausted sailors are stuck at sea." *The Wall Street Journal*. 2020. https://www.wsj.com/articles/ships-are-moving-but-exhausted-sailors-are-stuck-at-sea-under-coronavirus-restrictions-11586084402
[156] "Crew Changes: A humanitarian, safety, and economic crisis.' International Maritime Organization. 2021. https://www.imo.org/en/MediaCentre/HotTopics/Pages/FAQ-on-crew-changes-and-repatriation-of-seafarers.aspx
[157] ESCGS. Maritime Cyber Security White Paper: Safeguarding data through increased awareness. ESC Global Security Cyber Security White Papers. 2015.; Tam, Kimberly & Jones, Kevin. "Situational Awareness: Examining Factors that Affect Cyber-Risks in the Maritime Sector." International Journal on Cyber Situational Awareness, 4 (2020). 10.22619/IJCSA.2019.100125.
[158] John Frittelli. "Port and Maritime Security: Background and Issues for Congress." Congressional Research Service. Last Updated May 27, 2005. https://www.everycrsreport.com/reports/RL31733.html
[159] Aurora Almendral. "The Lonely and Dangerous Life of the Filipino Seafarer." *The New York Times*. 2019. https://www.nytimes.com/2019/11/30/world/asia/philippines-mariners-cargo-ships.html ; Costas Paris. "Ships are moving, but exhausted sailors are stuck at sea." *The Wall Street Journal*. 2020. https://www.wsj.com/articles/ships-are-moving-but-exhausted-sailors-are-stuck-at-sea-under-coronavirus-restrictions-11586084402
[160] "Shipping vessel crew member pleads guilty to drug trafficking." US Immigration and Customs Enforcement. 2020. https://www.ice.gov/news/releases/shipping-vessel-crew-member-pleads-guilty-drug-trafficking

line industry also sometimes reports incidents of rape, sexual assault, and suspicious deaths linked to crew members onboard.[161]

Cargo

As vessels transport larger amounts of containers, there are increased opportunities for smuggling and trafficking. These can occur due to the manipulation of cargo manifests, the transportation of dangerous goods, and the inability to process these increased volumes effectively.

Manifests. First, there is concern about preserving the legitimacy of cargo manifests. Since cargo manifests are digitized, malicious actors can hack into systems and change information about the contents of cargo manifests to facilitate smuggling.[162] This can allow the shipment of illicit goods with little detection.

Dangerous Goods. Another cargo problem is the shipment of dangerous goods. This cargo can increase the risk of a fire, explosion, or other incidents onboard a ship. For example, a fire erupted on the Maersk Honam in 2019 due to the improper handling of high-risk cargo.[163]An investigation determined that the improper labeling, handling, and storage of these goods on cargo ships contributed to the fire.[164] A survey by the National Cargo Bureau found that 4% of 31,000 containers (1,240) contained unsecured, dangerous cargo such as batteries, chemicals, or other flammable goods.

Cargo Volumes and Security Checks. A major emerging challenge for the MTS is the effective management of increased container shipping. Container volumes are exceeding security processing capabilities, creating potential blind spots.[165] "The number of containers handled by port terminals in 1993 doubled by 1998 and quintupled by 2008."[166] There is a concern that NSAs may exploit increased traffic flows to smuggle in small portions of illicit cargo piecemeal. This can make smuggling less detectable and harder to stop.[167]

On passenger vessels, there is also concern that current physical security checks may be insufficient to reduce the threat of a violent attack. In the United States, for example, passengers and vehicles are not required to be screened or searched before boarding a ferry.[168] After leaving the terminal, passengers are free to move throughout public areas on the vessel, including passenger and cargo areas.[169] Compared to cruise ships or airlines, ferries are expected to accommodate high volumes of traffic while operating within tight schedules, limiting the ability to carry out thorough checks of cargo, cars, and passengers.

---

[161] Catey Hill. "Do cruise lines have a crime problem?" Market Watch. 2014. https://www.marketwatch.com/story/do-cruise-lines-have-a-crime-problem-2014-02-21

[162] Rosehana Amin, Rory Duncan and Daniel Jones. "A very modern form of piracy: cybercrime against the shipping industry- part 1: rapidly developing risks." Clyde and Co LLP. 2021. https://www.lexology.com/library/detail.aspx?g=b4dc3b52-40b5-4700-afee-a95d09b7b6d3

[163] Costas Paris. "Ship Operators Raise Alarms Over String of Vessel Fires." Wall Street Journal. 2019. https://www.wsj.com/articles/ship-operators-raise-alarms-over-string-of-vessel-fires-11553425201?mod=article_inline

[164] Coastas Paris. "Spate of Fires Has Shipping Industry Looking at How Dangerous Goods are Handled." Wall Street Journal. 2019. https://www.wsj.com/articles/spate-of-fires-has-shipping-industry-looking-at-how-dangerous-goods-are-handled-11574600400

[165] Barbara-Anne Steegmu Johnson. "Transnational Terrorism: Globalization, Voluntary Compliance, and U.S. Port Security." The Global Studies Journal 5, no 4 (2015): 65-76. doi:10.18848/1835-4432/CGP/v05i04/40871

[166] Flynn, Stephen. "The Challenge of Securing the Global Supply System." MIT Press. 2020. P. 119.

[167] Eric L. Hampton. "Transnational Threats to Maritime Systems and Seaport Security." PhD Dissertation. Walden University. 2021. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=11702&context=dissertations

[168] Steven A. Blindbury. "Safe Seas: Protecting America's Ferries Against Criminal Mass-casualty Incidents." Journal of the NPS Center for Homeland Defense and Security 17. December 2018. p. 22. https://www.hsaj.org/articles/14937

[169] Ibid.

Domestic Ports

Domestic ports are vulnerable to attacks along several different vectors. Undetectable vessel traffic, port congestion, aging infrastructure, and the adoption of automated port systems arose in conversations as some of the most likely reasons an attack could materialize.

Ships

Small Vessel Traffic. Several interviewees cited small vessel traffic within and around ports as an increasingly pressing concern. A small vessel refers to any watercraft less than 300 tons, typically including fishing boats, tug boats, and recreational vehicles. A lack of regulation and monitoring makes the maritime space vulnerable to undetected maneuvering and illicit trafficking by small vessels.

Due to their size and anonymity, small vessels can move around undetected, increasing the risk of a physical attack or smuggling. Some ports use long-range tracking systems and shore-based radar systems to detect small vessel traffic, but these are not widely deployed. While the USCG tries to regulate traffic into main shipping channels, "small vessels can and often do violate these rules to traverse or even congregate in main shipping channels."[170] Another blind spot identified in interviews is the difficulty of monitoring small vessel traffic. While large vessels have Automatic Identification System (AIS) requirements to facilitate tracking, small vessels do not. This allows small vessels to move around ports undetected and enter unauthorized areas.

The attack against the *USS Cole* is probably the most prominent small vessel attack to date. However, small vessels can also enable smuggling. Between 2012 and 2018, the rate of small vessels used in drug trafficking increased by 300%.[171] There are further reports of small vessels being used to facilitate hijacking, piracy, and terrorist attacks on water.[172] The most serious risk associated with small vessel traffic is that it could be used to smuggle in nuclear materials.

To manage these risks, DHS published a Small Vessel Security Strategy in 2008, but interviewees noted that it had not been implemented to the full extent possible.[173] Following the 2002 MTSA, the federal government implemented new requirements for vessel operators to report to CBP when they return from foreign ports. However, there is a low level of compliance with this requirement due to a lack of advertising of this requirement and a lack of personnel to conduct these inspections.[174]

Port Congestion. While growing levels of container shipping already raised the risk of port congestion, but the COVID-19 pandemic's effect on supply chains has exacerbated this risk. Port congestion when vessels are unable to load or unload upon arrival. Instead, vessels typically sit in anchorages or drift boxes until there is space in port to move. For example, a record of 46 vessels were waiting to enter the Ports of Los Angeles and Long Beach due to an increase in for imported goods concurrent with COVID-related labor shortages and operational restrictions.[175] Port congestion creates several losses, including shipping delays, higher inventory

[170] Christine Hanson. "The Small Vessel Threat and Related GAO Products." Transportation Research Board Marine Board Spring Meeting. 2011. Washington, DC. http://onlinepubs.trb.org/onlinepubs/mb/Spring2011/6.2_Hanson.pdf
[171] "The Number of Small Fishing Vessels Smuggling Illegal Drugs Has Tripled." Smithsonian Magazine. 2020. https://www.smithsonianmag.com/science-nature/number-small-fishing-vessels-smuggling-illegal-drugs-has-tripled-180976157/
[172] "DHS Could Benefit from Tracking Progress in Implemnting the Small Vessel Security Strategy." General Accounting Office. 2013. https://www.gao.gov/assets/gao-14-32.pdf
[173] "Small Vessel Security Strategy." Department of Homeland Security. 2008. https://www.dhs.gov/xlibrary/assets/small-vessel-security-strategy.pdf
[174] "DHS Could Benefit from Tracking Progress in Implementing the Small Vessel Security Strategy." General Accounting Office. 2013. https://www.gao.gov/assets/gao-14-32.pdf
[175] Will Feuer. "Record number of container ships waiting off California coast." *New York Post.* August 31, 2021. https://nypost.com/2021/08/31/california-has-record-number-of-container-ships-waiting-off-coast/

costs, and higher demurrage costs. Forcing vessels to sit in steerage makes them vulnerable to a physical attack by allowing NSAs to gather intelligence and learn more about these vessels. Congestion also raises the risk of accidents.[176] Finally, congestion can put pressure on dockworkers and other terminal operators to expedite unloading and loading procedures. This can make it easier to smuggle illegal cargo.[177]

Container Shipping Size. A final vulnerability within ports stems from the increased size of container ships. Vessels have grown larger over the last twenty years to handle increased container shipping traffic. The widening of the Panama Canal and dredging of ports around the United States have increased capacity for large neo-Panamax vessels that can transport at least 10,000 TEU. A concern is that larger ships will exacerbate port congestion issues, magnifying the risk of a TSI.[178] Larger ships are also more challenging for harbor pilots to navigate, increasing the likelihood of an accidental collision or physical damage.[179] For example, in 2019, two bulk carriers collided in Vancouver's Inner Harbor. The Transportation Safety report attributed the incident to a lack of situational awareness and poor communication.[180]

Physical Infrastructure

A second set of factors that make domestic ports vulnerable to cyber threats, advanced weapon systems, and violent extremism concern the state of port infrastructure. Interviewees expressed fears that inconsistent physical security protections and aging infrastructure increased susceptibility to attacks.

Inconsistent Physical Security Protections. There are two types of ports: operational and landlord ports. Operational ports are publicly owned and operated, such as the Ports of Savannah, Charleston, and Boston. The port authority oversees both the construction and operations of a given port. In contrast, landlord ports lease out wharves to terminal operators, which then privately handle cargo operations and transportation. These ports include the Ports of Los Angeles, Oakland, and Miami.[181]

Over the last 40 years, there has been a growth in landlord ports. This can amplify the unique security risks associated with landlord ports. Since terminal operators control individual access to their areas of operations, there are multiple ways for an intruder to enter the port. "The port is wide open, lacking a single gate that everyone enters and exits."[182] If port access is diffused across multiple points of entry, it can be easier for a single actor to slip into any one gate.[183] These physical security issues may explain, in part, there has been an increase in reports of security breaches and suspicious activity since 2003. [184]

Unauthorized Port Access. Another physical security risk is unauthorized access to the port. Workers require a Transportation Worker Identification Credential (TWIC) to gain access to a port.[185] However, a 2016 audit

---

[176] Keith Wallis. "Yantian port disruption impact widens as delays lengthen." Journal of Commerce Online. 2021. https://www.joc.com/port-news/international-ports/yantian-port-disruption-impact-widens-delays-lengthen_20210603.html

[177] "Port Congestion Creates Security Threats." National Threat Initiative. 2004. https://www.nti.org/gsn/article/port-congestion-creates-security-threats/

[178] Bill Mongelluzzo. "Increasing vessel size a red flag for US ports." Journal of Comerce Online. 2020. https://www.joc.com/maritime-news/container-lines/increasing-vessel-sizes-red-flag-us-ports_20201221.html

[179] "Ship Navigation in Harbors: Safety Issues." Congressional Research Services. 2008. https://www.everycrsreport.com/files/20080208_RL34365_f73a60b7cbd5c185f19541ad94167176d137e48c.pdf

[180] David Ball. "Ship crash in Vancouver harbour blamed on `systematic failure,' communications `breakdown.' CBC News. 2021. https://www.cbc.ca/news/canada/british-columbia/ship-collision-2019-transportation-safety-board-report-1.6104556

[181] "Ports Primer: 3.1 Port Operations." United States Environmental Protection Agency. N.d. https://www.epa.gov/community-port-collaboration/ports-primer-31-port-operations

[182] Ed Finkel. "Ports Fight Security Breaches and Possible Funding Reductions." Security Magazine. 2018. https://www.securitymagazine.com/articles/88851-ports-fight-security-breaches-possible-funding-reductions

[183] Ibid,

[184] Eric L. Hampton. "Transnational Threats to Maritime Systems and Seaport Security." PhD Dissertation. Walden University. 2021. P. 64. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=11702&context=dissertations

[185] See Section 1 in this report for an overview of the TWIC program.

follow that the TSA's Office of Intelligence and Analysis has "not provided sufficient oversight and guidance over the TWIC Program," leading to ineffective fraud detection techniques, a lack of guidance, gaps in quality controls, and insufficient planning for recurrent vetting.[186] Similarly, an audit by the Justice Department found that there are "deficiencies" in the FBI sharing intelligence to the TSA regarding watchlisted individuals when they apply for or renew a TWIC; between October 2006 and January 2017, there were 214 incidents of FBI-watch-list individuals who either held or applied for a TWIC, including some with a No Fly status.[187] These results all reduce the quality of TSA's background check and TWIC application processes, creating a risk that unauthorized personnel could access secure areas of maritime facilities.

Aging Infrastructure. Despite a number of modernization efforts undertaken at ports and inland waterways over the last few years, there are concerns these efforts may be insufficient to reduce the risk of an attack. Aging infrastructure problems increase port vulnerability in at least two ways.

First, aging infrastructure is susceptible to more frequent outages and maintenance. Over the last 20 years, lock outages have increased due to a growing number of scheduled and unscheduled maintenance issues.[188] Between 2015-2019, 63% of lock closures were caused by unplanned maintenance.[189] Much of this problem is because many locks, dams, and inland waterways were built decades ago. When these systems need repair, it can create massive delays in shipping, increase the costs of shipping, and also force existing vessels to slow down or stop their travels.[190] In 2019, lock damage at the Bonneville Dam on the Columbia River closed for three weeks, stalling fourteen commercial vessels.[191] This can increase the visibility of vessels en route and make them targets for interdiction.

Second, aging infrastructure exacerbates congestion problems. Many ports and waterways were not originally designed to handle the levels of shipping traffic seen today. Some efforts—like dredging a port to make it deeper—have helped ports accommodate larger vessels.[192] However, these efforts cannot handle congestion. Prior to the pandemic, experts predicted that the Upper Mississippi River and Illinois Waterway system would reach 90% of its annual throughput capacity by 2020.[193]

Poor Investment in Maintenance and Modernization. To address aging infrastructure concerns, policymakers recommend increased investment in maintenance and modernization efforts. However, a significant gap exists between what practitioners agree is necessary and what is currently available. Currently, maritime infrastructure receives funding from the Inland Waterway Trust Fund (IWTF) and the Harbor Maintenance Trust Fund (HMTF). The HMTF is a relatively reliable source of revenue because it imposes a small maintenance tax on

---

[186] "TWIC Background Checks are Not as Reliable as They Could Be." Office of the Insepector General U.S. Department of Homeland Security. September 1, 2016. p. 5. https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-128-Sep16.pdf
[187] "Audit of the Federal Bureau of Investigation's Management of Maritime Terrorism Threats." Office of the Inspector General U.S. Department of Justice. March 2019. p. 10-11. https://oig.justice.gov/reports/2019/a1918.pdf
[188] "Inland Waterways and Export Opportunities." US Army Corps of Engineers Institute for Water Resources. 2013. https://www.lrd.usace.army.mil/Portals/73/docs/Navigation/PCXIN/Inland_Waterways_and_Export_Opportunities-FINAL_2013-01-03.pdf
[189] "Inland and Intracoastal Waterways: Primer and Issues for Congress." Congressional Research Service. 2020. https://crsreports.congress.gov/product/pdf/IF/IF11593
[190] "Inland Waterways: Actions Needed to Increase Budget Transparency and Contracting Efficiency." General Accounting Office. 2018. https://www.gao.gov/products/gao-19-20
[191] Matthew Weaver."Bonneville Dam lock repairs keep barges on hold." Daily Astorian. 2019. https://www.dailyastorian.com/news/bonneville-dam-lock-repairs-keep-barges-on-hold/article_369e4fc4-d457-11e9-bed5-b7f01ac9cd3d.html
[192] Michael Angell. "Dredging to boost vessel size limit for Port of New Orleans." Journal of Commerce Online. 2020. https://www.joc.com/port-news/us-ports/dredging-boost-vessel-size-limit-port-new-orleans_20200804.html
[193] Rob Bailey and Laura Wellesly. "Chokepoints and Vulnerabilities in Global Food Trade." Chatham House. 2017. https://www.chathamhouse.org/sites/default/files/publications/research/2017-06-27-chokepoints-vulnerabilities-global-food-trade-bailey-wellesley-final.pdf

imported cargo.[194] As imports increase, so does the Harbor Maintenance Fund. However, the IWTF tends to carry a "zero balance" because it is tied to the $0.29 federal gas tax.[195] The IWTF fund struggles to finance all necessary maintenance and replacement operations because these costs have not kept pace with inflation, and the number of general fund projects is increasing.[196] The American Society of Civil Engineers predicts that this will result in a funding gap of $24.8 billion between 2020-2029.[197] This investment gap means these infrastructure vulnerabilities will, at best, persist for some time and, at worst, grow increasingly dire.

Physical-Cyber Ties. As ports become increasingly interconnected, they rely more on a physical-cyber interchange. This means that physical infrastructure is reliant on digital systems to coordinate and keep systems operational. A key vulnerability within this physical-cyber interchange is the ability for cyber- attacks to physically disable port operations. For example, a denial-of-service attack could bring down port power systems and intercept backup systems from going into effect.[198] Researchers at the University of Plymouth Maritime Cyber Threats Research Group replicated and extended a scenario based on the 2015 cyber-attack on the Ukraine power grid (see Box 7). The Ukraine attack lasted approximately six hours, but control centers were still not fully operational two months after the attack.[199] A concern is that hackers could time the power grid outage to turn off cranes and delay port turnaround times. Another concern is that hackers could use a slightly more sophisticated form of malware to cause physical damage to parts of a power grid such as a transformer. They could manipulate the Uninterruptable Power Supply (UPS) back-up systems to turn off redundancy systems. If successful, a down power transformer could shut down a port from several days to up to several months.[200]

Box 7. 2015 Ukraine Cyber Power-Grid Attack
On December 23, 2015, hackers infiltrated the Prykarpattyaoblenergo power grid control center in the Ivano-Frankivsk region of Ukraine. Hackers gained access to the information control systems, turned off the power breakers, and disrupted the power supply for six hours. Hackers also reconfigured the power grid's Uninterruptable Power Supply to prevent backup power from turning on. To accomplish this attack, hackers exploited a vulnerability in Microsoft Word using the BlackEnergy3 trojan. Using a basic phishing email, they attached a malicious Word document which remote workers unsuspectingly opened. The hackers used this malware to collect worker credentials when they logged onto the Supervisory Control and Data Acquisition (SCADA) system so they could gain access to the main power supply.

Digital Infrastructure

Automated Systems and Smart Ports. In order to manage higher levels of container traffic, ports increasingly rely on automated systems. These "smart ports" can more efficiently handle container movement and optimize

[194] Bryce Campanelli. "A Deep Dive on America's Ports." Bipartisan Policy Center. 2017. https://bipartisanpolicy.org/blog/a-deep-dive-on-americas-ports/
[195] "Inland Waterways and Export Opportunities." US Army Corps of Engineers Institute for Water Resources. 2013. https://www.lrd.usace.army.mil/Portals/73/docs/Navigation/PCXIN/Inland_Waterways_and_Export_Opportunities-FINAL_2013-01-03.pdf
[196] "Inland and Intracoastal Waterways: Primer and Issues for Congress." Congressional Research Service. 2020. https://crsreports.congress.gov/product/pdf/IF/IF11593
[197] "Failure to Act: Ports and Inland Waterways – Anchoring the US Economy." American Society of Civil Engineers. January 2021. https://infrastructurereportcard.org/wp-content/uploads/2020/12/failure-to-act-2021-ports-inland-waterways.pdf
[198] Kimberly Tam and Kemedi Moara-Nkwe and Kevin Jones. "A Conceptual Cyber-Risk Assessment of Port Infrastructure. 2021." World of Shipping Portugal. An International Research Conference on Maritime Affairs, January 28-29 2021, Virtual Conference, Parede, Portugal.
[199] Kim Zetter. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired Magazine. 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
[200] Kimberly Tam and Kemedi Moara-Nkwe, and Kevin Jones. "A Conceptual Cyber-Risk Assessment of Port Infrastructure. 2021." World of Shipping Portugal. An International Research Conference on Maritime Affairs, January 28-29 2021, Virtual Conference, Parede, Portugal.

transportation. They are also seen as a tool to curb smuggling by adopting blockchain systems to provide virtual ledgers and real-time cargo monitoring.[201]

These smart ports leverage the Internet of Things (IoT), or the network systems at ports that can all access a common server and speak to each other. For example, automated mooring systems can speak with terminal computer systems to ensure a vessel comes into port safely and efficiently.[202] A crane can use an optical character recognition (OCR) camera to scan a container and offload it to the correct location in the container yard more rapidly.

Interviewees stressed that automation not only increases a port's susceptibility to cyber-attacks, but also harms a port's ability to maintain continuity of operations should systems go offline. A number of automated port systems are vulnerable to interference and degradation, including:

- Voice Over Internet Protocol (VoIP): VoIP facilitates telecommunications. In ports, a VoIP system typically governs how a trucker checks into a terminal and gains access. The main concern is that non-state actors could manipulate a VoIP system to gain unauthorized access into a port location.[203]
- Cargo Manifests: Non-state actors can hack into port systems, and change information about the contents of cargo manifests to facilitate smuggling.[204]
- Cargo Locations: Non-state actors can hack into port systems to recover information about the location and security level of different containers within a port. For example, the Port of Antwerp uncovered a two-year drug trafficking operation in 2013 that used this system.[205]
- OCR Readings: Cranes currently have OCR cameras on board to identify containers. Port operations aim to optimize crane rates to scan containers on a ship as quickly as possible. However, if a port network is degraded, then this could affect the crane's processing rate. It could delay container transportation and increase port congestion.
- Security Cameras: There is a similar risk to security systems in ports as onboard vessels. In addition to the risk of physical blind spots—locations that cameras cannot observe—there is a possibility that non-state actors may hack into security cameras in order to pivot cameras away from nefarious activities.
- Vessel Traffic Systems (VTS): Vessels increasingly rely on shore-based control systems to guide ships safely as they approach a port. However, malicious actors could manipulate VTS systems to direct ships into dangerous situations or misdirect them to other locations where interception is easier.[206]

Network Security. The adoption of new and increasingly interconnected digital systems makes ports more vulnerable to large-scale attacks. Port partners used to have more isolated systems known as point-to-point systems. When one system went down, the effects were relatively isolated. However, port networks now operate as part of a large hub-and-spoke model. In this model, actors all access a shared central network. An attack against any part of the network has the opportunity to contaminate the whole network and bring it down. In other words, the network model carries a risk of substantial cascading effects. Attacks on any part of the network can disable larger sections of a port than a traditional point-to-point model.

---

[201] Sae-Jin Park. "Busan selected in state project to establish smart logistics port system." Aju Business Daily. 2020. http://www.ajudaily.com/view/20200706091846830

[202] "Smart Ports in the Pacific." Asian Development Bank. November 2020. https://www.adb.org/sites/default/files/publication/646401/smarts-ports-pacific.pdf

[203] Gabe Weaver. "Assessment and Measurement of Port Disruptions." Critical Infrastructure Resilience Institute. University of Illinois. 2018. https://ciri.illinois.edu/events/assessment-and-measurement-port-disruptions

[204] Rosehana Amin, Rory Duncan and Daniel Jones. "A very modern form of piracy: cybercrime against the shipping industry- part 1: rapidly developing risks." Clyde and Co LLP. 2021. https://www.lexology.com/library/detail.aspx?g=b4dc3b52-40b5-4700-afee-a95d09b7b6d3

[205] Tom Bateman. "Police warning after drug traffickers' cyber-attack." BBC. 2013. https://www.bbc.com/news/world-europe-24539417

[206] Rosehana Amin, Rory Duncan and Daniel Jones. "A very modern form of piracy: cybercrime against the shipping industry- part 1: rapidly developing risks." Clyde and Co LLP. 2021. https://www.lexology.com/library/detail.aspx?g=b4dc3b52-40b5-4700-afee-a95d09b7b6d3

For example, AT&T installed Multiprotocol Label Switching (MPLS) in some ports as a routing technique in telecommunications networks.[207] The MPLS directs data from one node to the next based on short path labels rather than long network addresses. This network decision is advantageous in avoiding complex lookups in a routing table and speeding traffic flows. The main change this had was that networks are now fiber-connected. The advantage is that if one server goes down, the remaining servers stay up, preserving port resiliency The disadvantage is that the ties make everyone susceptible to the same cyber-attacks. If one node is disabled, then all the others can become infected and be impacted.

Similarly, the IoT has created a multitude of entry points for cyber threats to compromise network security. The adoption of IoT or other technology for automation has outpaced the systems and processes implemented to protect these devices and their users. Interconnected devices allow a virus or worm to spread through a network of devices and multiply an attack's impact. For example, Zscaler, an American cloud-based information security company, analyzed over 575 million device transactions and 300,000 IoT-specific malware attacks blocked by the company over two weeks in 2020.[208] These attacks—which increased by 700% compared to pre-pandemic levels—targeted 553 different device types, including printers, digital signage, and smart TVs, which were connected to and communicating with corporate IT networks.[209] 76% of these devices communicated on unencrypted plain text channels, illustrating the risks businesses face when using unprotected and interconnected IoT devices.[210]

Overreliance on Digital Systems. A final concern that stakeholders associated with a port's digital infrastructure suggested stakeholders rely too heavily on these automated systems and put too much "trust" in systems. Artificial intelligence, machine learning, and predictive analytics can enhance current port operations and make them more efficient. However, there is a fear that these can come at a loss of human discretion and flexibility in responding to incidents. If operators become too reliant on the systems, then they may lose institutional expertise to maintain continuity of operations if systems go offline. This could prolong a port's closure and aggravate the effects of this disruption. One interviewee noted that the best way to handle this—and other network security concerns—is to build in as many redundant systems as possible.

People

Companies and Organizational Culture

Insular Culture. Some interviews mentioned the insular organizational culture around ports as a potential liability. The concerns here stressed how a closed culture impeded information-sharing, especially around potential vulnerabilities. For example, between 2017-2020, there was a 900% increase in maritime cyber-attacks.[211] However, this is likely an undercount of the true number of incidents. Companies often do not disclose incidents due to fears reporting will hurt their current contracts, stock valuations, or legal liability.[212] Although the Securities and Exchange Commission encourages companies to make "timely" disclosures, there

[207] "Minutes of the 178th Committee Meeting of the LA/LB Harbor Safety Committee." Marine Exchange of Southern California. February 5, 2020. https://mxsocal.org/assets/pdf/hsc/minutes/178-hsc-mtg-feb-5-2020.pdf
[208] "Zscaler Study Confirms IoT Devices A Major Source of Security Compromise, Reinforces Need for Zero Trust Security." Zscaler ThreatLabz. July 15, 2021. https://www.zscaler.com/press/zscaler-study-confirms-iot-devices-major-source-security-compromise-reinforces-need-zero
[209] Ibid.
[210] Ibid.
[211] "Maritime Cyber Attacks Increase by 900% in the last three years." Marine Insight. 2020. https://www.marineinsight.com/shipping-news/maritime-cyber-attacks-increase-by-900-in-three-years/#
[212] Eamon Javers. "Cyberattacks: Why Companies Keep Quiet." 2013. https://www.cnbc.com/id/100491610

is currently no legal mandate to report these incidents.[213] This allows these threats to penetrate and operate in company networks undetected for far too long (See Box 9).[214]

Broader research shows that insular cultures can also make it hard to voice concerns or challenge conventional procedures.[215] Research on operations at the Port of Rotterdam and Port of Hamburg found that internal cultures led to the "commercialization" of policing, wherein preserving commercial activity tended to override security and protective measures. As a direct result, security officers within the port perceived their role as insignificant and felt powerless to effectuate change. If security officers are unable to implement necessary policies, then malicious actors may exploit this to stage an attack.[216]

Insular cultures can also create low morale among workers and internal divisions. Existing research on organizational learning suggests that if these issues are left unaddressed, then inaction could raise the risk of another surprise attack.[217]

Growing Stakeholders and Divergent Priorities. A similar organizational culture problem is the number of stakeholders. As port operations increase, the number of stakeholders has also risen. This growth can raise the risk of an attack by creating a collective action problem in risk management. Many emerging threats are highly complicated and multi-dimensional. Organizing an effective and coordinated response depends, in part, on how well different stakeholders can work together to manage the risk.

In the cyber domain specifically, there is no comprehensive cyber strategy that establishes a common framework for industry and government stakeholders. One interviewee expressed that existing cyber defense strategies outlined by the Cybersecurity & Infrastructure Security Agency (CIPA) are not adequately linked to the operations of companies in the maritime industry. This lapse in government-industry coordination has led to the common use of outdated and ineffective IT systems, including brittle firewalls and security software. For example, in 2019, malware compromised the functionality of the onboard computer system of a vessel traveling to the Port of New York and New Jersey. Although the ship's essential control systems were not affected, an inter-agency investigation found that the vessel was operating without effective cybersecurity measures.[218] Without a shared approach to the cyber domain, companies voluntarily adopt cyber hygiene standards "out of sheer survival."[219]

Governance and Management Challenges. Competing resources and priorities can create governance and management challenges at ports. Various state and local public entities govern MTS ports, including port authorities, port navigation districts, and municipal port departments. Meanwhile, different companies may own a ship's cargo while another manages its operation. At the same time, countries have specific laws and regulations for both ships and ports within their territory.

Inconsistencies in ownership, operational procedures, security protocols, and technological capability make it challenging to integrate cyber risk management throughout the MTS and the global supply chain. Results from

[213] Craig Newman. "When to Report a Cyberattack? For Companies, That's Still a Dilemma." New York Times. 2018. https://www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html
[214] Swinhoe, Dan. "Why Businesses Don't Report Cybercrimes to Law Enforcement." CSO Online. International Data Group. 2019. https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html
[215] Wilensky, Harold L. Organizational intelligence: Knowledge and policy in government and industry. Vol. 19. Quid Pro Books, 1967.
[216] Eski, Yarin (2020) Customer is king: promoting port policing, supporting hypercommercialism, Policing and Society, 30:2, 153-168, DOI: 10.1080/10439463.2019.1606808
[217]Garicano, Luis, and Richard A. Posner. "Intelligence failures: An organizational economics perspective." Journal of Economic Perspectives 19, no. 4 (2005): 151-170; Zegart, Amy. "9/11 and the FBI: The organizational roots of failure." Intelligence and National Security 22, no. 2 (2007): 165-184.
[218] James Rundle. "U.S. Coast Guard Warns Shipping Industry on Cybersecurity." *The Wall Street Journal*. July 11, 2019. https://www.wsj.com/articles/u-s-coast-guard-warns-shipping-industry-on-cybersecurity-11562837402?mod=article_inline
[219] Interview.

one survey of over 20,000 marine professionals found that "a lack of consistency" between stakeholders "makes it difficult for shipping companies to set up their own internal approach to safety assurance" against cyber-attacks, and that there is "further uncertainty about the effectiveness and appropriateness of voluntary standards and mandatory regulations to tackle the problem."[220] Conflicting organizational cultures, regulations, and resources have led aspects of port security to be compartmentalized across the industry.

Operators

Foreign Operators. Over the last 40 years, there has been a growth in landlord ports. As part of this, foreign operators have become stakeholders in an increasing number of U.S. ports. By 2006, foreign companies managed 80% of terminals in the United States.[221] A key concern is whether the growth in foreign terminal operators presents a new vulnerability to port security. Some argue that foreign ownership creates new counterterrorism vulnerabilities for four reasons:

- Foreign operators may gather intelligence about standard operating procedures and security measures, which could then be exploited to stage an attack[222]
- Foreign operators may not comply with existing verification regimes, which could raise the risk of smuggling or transporting illicit goods[223]
- Foreign operators may undermine existing IT infrastructure and communication technologies by being on the same network, which creates opportunities for subterfuge and infiltration[224]
- Foreign operators could use their influence to have companies servicing US national security interests re-prioritize contracts or slow down resupply operations[225]

Since 2006, Chinese state-owned enterprises like COSCO and China Merchants have expanded their control over foreign ports. This rapid expansion is part of President Xi Jinping's "Maritime Silk Road" strategy, which aims to complement the Belt and Road Initiative on-land by increasing Chinese influence in foreign ports. By 2017, Chinese operators ran 29 ports in 15 countries and 47 terminals in 13 countries.[226] By 2020, this had expanded to 26 ports in 18 countries. China's role in these ports is debated. Some argue it is primarily commercial and an attempt to expand Chinese economic influence.[227] Others view cases like the Port of Djibouti, where China Merchants has a majority stake in the main port and thus "handles nearly all the incoming supplies for [peacekeeping and military] bases," as a source of alarm for the United States and its allies.[228] Foreign influences at domestic ports and at ports in major trading partners seem likely to continue.

---

[220] Kevin Tester. "Technology in shipping The impact of technological change on the shipping industry." Clyde & Co and the Institute of Marine Engineering, Science, and Technology. November 2017. p. 11. https://www.imarest.org/policy-news/thought-leadership/1010-technology-in-shipping/file

[221] Adam Davidson. "Most US Port Terminals are Foreign-Run." NPR. 2006. https://www.npr.org/templates/story/story.php?storyId=5234177

[222] John Frittelli and Jennifer Lake. "Terminal Operators and their role in US Port and Maritime Security." Congressional Research Service. 2007. https://www.everycrsreport.com/reports/RL33383.html#_Toc216485534

[223] "National Security Implications of the Dubai Ports World Deal to Take Over Management of US Ports." Hearing Before the Committee on Armed Services. House of Representatives. 109th Congress. March 2, 2006. US GPO: Washington. https://www.govinfo.gov/content/pkg/CHRG-109hhrg32987/html/CHRG-109hhrg32987.htm

[224] "China's Maritime Silk Road Initiative: Implications for the Global Maritime Supply Chain." Hearing Before the Subcommittee on Coast Guard and Maritime Transportation of the Committee on Transportation and Infrastructure. House of Representatives. 116th Congress. October 7, 2019. US GPO: Washington. https://www.govinfo.gov/content/pkg/CHRG-116hhrg41367/html/CHRG-116hhrg41367.htm

[225] Ibid.

[226] Wade Shepard. "China's Seaport Shopping Spree: What China is Winning by Buying up the World's Ports." *Forbes*. 2017. https://www.forbes.com/sites/wadeshepard/2017/09/06/chinas-seaport-shopping-spree-whats-happening-as-the-worlds-ports-keep-going-to-china/?sh=1178f3824e9d

[227] Matthew Funaiole and Jonathan Hillman. "China's Maritime Silk Road Initiative: Economic Drivers and Challengers." Center for Strategic and International Studies. 2018. https://www.csis.org/analysis/chinas-maritime-silk-road-initiative-economic-drivers-and-challenge

[228] "China is making substantial investment in ports and pipelines worldwide." *The Economist*. 2020. https://www.economist.com/special-report/2020/02/06/china-is-making-substantial-investment-in-ports-and-pipelines-worldwide

Box 8. Dubai Ports World
The Dubai Ports (DP) World controversy in 2006 captured many concerns surrounding foreign influences in domestic ports. That year, the United Arab Emirates DP World acquired a British-owned Peninsular and Oriental Steam Navigation Company (P&O). This purchase meant DP World also gained control over container terminals in six US ports: Baltimore, Miami, New Orleans, New York, New Jersey, and Philadelphia. It would also have partial operational control over 16 ports. Although the Committee on Foreign Investment to the United States (CFIUS) approved the acquisition, Congress and public outcry blocked the deal on the belief that the UAE had tenuous ties to Al Qaeda. Increasing UAE's control over US ports could increase the risk of illicit trafficking or terrorist activity inside the US borders. Eventually, the acquisition failed due to public scrutiny.

Longshore and Dockworkers

Labor Shortages. Similar to crew shortages onboard vessels, the COVID-19 pandemic exacerbated labor shortages at domestic ports. Interviewees suggested that labor shortages can generate unexpected security risks by, for example, hiring replacements without full vetting under the TWIC Maritime Program Management Office and training by port operators. Hasty hiring can increase the risk of accidental collisions, mishandled cargo, or inadequate situational awareness. There is a separate risk that longshoremen and labor unions could pose a threat to smart ports. As ports become increasingly automated, this could displace port workers from their traditional livelihoods. This could seed grievances that raise the likelihood of an insider threat.

Poor Vetting. Even in cases where port operations hire qualified staff, there are concerns of proper vetting. Although the MTSA implemented protocols requiring valid credentials and authorization, these protocols are sometimes subverted or ignored. "Maritime staff and contractors are not always fully vetted, particularly when positions are filled overseas. In the more extreme cases, they may be mentally ill, violent ex-felons, or even terrorists, serving in various posts such as merchant mariners, longshoremen, and tractor-trailer drivers."[229] Insider threats may gain access to terminal operating systems, access control measures, or cargo management systems. Authorized access allows insiders to potentially move containers to areas with less camera coverage or manipulate seals to import illicit materials.[230] NSAs, especially transnational criminal organizations, often use low-paid supply chain workers to infiltrate and move cargo around seaports.[231] In a case study of operations around the Port of Rotterdam, Eski and Buijt (2017) show that TCOs use port employees to breach security seals, deliberately reposition containers, and share credentials with unauthorized users to facilitate drug trafficking.[232]

[229] Marie-Helen Maras and Lauren R. Shapiro. 'On a Sea of Risk." ASIS Online. 2018. https://www.asisonline.org/security-management-magazine/articles/2018/04/on-a-sea-of-risk/
[230] Eric L. Hampton. "Transnational Threats to Maritime Systems and Seaport Security." PhD Dissertation. Walden University. 2021. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=11702&context=dissertations
[231] Michael H. Belzer and Peter F. Swan. (2011). Supply Chain Security: Agency Theory and Port Drayage Drivers. *The Economic and Labor Relations Review* 22, no. 1. 2011. p. 41–63.
[232] Yarin Eski and Romano Buijt. "Dockers in drugs: Policing the illegal drug trade and port employee corruption in the Port of Rotterdam." *Policing*: *A Journal of Policy and Practice* 11, no. 4 (Nov 2016). https://doi.org/10.1093/police/paw044

Box 9. Quality of Frontline Policing and Security at the Ports of Rotterdam and Hamburg
The Ports of Rotterdam and Hamburg are crucial transit junctions for people and goods traveling within Europe and to other parts of the world. Security is central to ensuring the flow of commerce and people without disruption. Therefore, it is important to assess the quality, experiences, and expertise of frontline port security facilities and employees in these opaque and highly securitized locations.

An ethnographic study carried out from 2010 and 2016 at the Ports of Rotterdam and Hamburg disclosed several conclusions on the state of port security. The author found that hyper-commerciality and corporate power greatly affected transport policing. Frontline employees expressed that port policing had become managerialized and corporatized. Higher-up managers were viewed as inept due to their lack of on-the-ground policing knowledge and aggressively market-oriented policies. Such distrust and disunity among and between managers and port security staff can create unintended gaps in port security.

Participants also experienced a sense of insignificance and meaninglessness in frontline policing work. The author summarizes that "the mass-scaling, digitalization, and professionalization of the port and port theft have led to feelings of policing an unfamiliar, anonymized other that is obscure and unpredictable, and in their imagination and practice, non-existent."[233] Participants felt that hyper-commercialization of maritime trade had led to the commercialization of their work for marketing purposes while sensing that they are not actually effective within the current threat environment.

In a related study, the author revealed some insight into the cases where frontline port security employees become "insider threats."[234] The authors analyzed 22 cases in which 51 employees of the Port of Rotterdam had a role in trafficking drugs in port containers. The most common reasons why individuals become involved in drug trafficking were: addiction to drugs, gambling, or other addictive habits which had caused financial hardship; financial hardship within the family or extended family; and being co-opted by a colleague. Overall, these findings point to the role of personal circumstances and social ties in port criminality.

Law Enforcement

Law enforcement operations at ports may be inadequate to detect and deter threats due to understaffing, resource acquisition delays, operational predictability, and poor information sharing. In each case, existing procedures may create barriers to respond to an incoming threat swiftly and effectively. These slow response times can undercut detection, deterrence, and mitigation capabilities.

Under-Staffing. Law enforcement operations at ports may first be inadequate to detect and deter threats due to understaffing. Increased traffic is overstretching the operational capacity existing port workers. They cannot assess all incoming containers, which allows drugs to be smuggled in more easily.[235] Although the CBP and USCG try to optimize their resources given constraints, they often find themselves "terribly understaffed," which makes it hard to adequately address all the issues related to smuggling. The CBP loses approximately 700 staff per year and finds itself short of personnel.[236]

---

[233] Yarin Eski. "Customer is king: promoting port policing, supporting hypercommercialism." *Policing and Society: An International Journal of Research and Policy* 30, no. 2 (April 2019). https://doi.org/10.1080/10439463.2019.1606808
[234] Yarin Eski and Romano Buijt. "Dockers in drugs: Policing the illegal drug trade and port employee corruption in the Port of Rotterdam." *Policing*: *A Journal of Policy and Practice* 11, no. 4 (Nov 2016). https://doi.org/10.1093/police/paw044
[235] Costas Paris. "Global Shipping Faces Troubling New Smuggling Questions." *The Wall Street Journal*. 2020. https://www.wsj.com/articles/global-shipping-faces-troubling-new-smuggling-questions-11578330634
[236] Ed Finkel. "Ports Fight Security Breaches and Possible Funding Reductions." Security Magazine. 2018. https://www.securitymagazine.com/articles/88851-ports-fight-security-breaches-possible-funding-reductions

Resource Acquisition Delays. A second law enforcement concern related to operational preparedness was slow resource acquisition times. Interviewees suggested that the processes currently used to adopt new technologies into existing operational procedures are overburdened by bureaucracy. While these standards exist to mitigate national security risks to adoption, there is a concern that this framework is obsolete and overly cumbersome when dealing with the risks posed by emerging technologies.[237] Without new technologies, interviewees suggested that it is hard to remain competitive in detecting and deterring non-state actor attack innovations. For example, counter-UAS technology may become ineffective to counter unmanned systems because non-state actors adopt and use newer, more sophisticated technology faster than USCG can adapt.[238] Delayed access to new technologies and methods could impede law enforcement's ability to detect and disrupt threats.

Reverse Machine Learning. A third vulnerability for law enforcement is the potential for "reverse machine learning." The risk is that port operations, vessel traffic, and safety protocols are highly routine and standardized. Training exercises, patrols, and other security protocols are rehearsed and executed with a high level of predictability. This allows NSAs to observe and collect data about the timing, location, and type of activity carried out across a port. If desired, NSAs could use this information to predict where USCG is most likely to carry out patrols or when containers are most vulnerable to interception. This reverse ML endeavor could help malicious actors carry out activities without being caught.

Incomplete Information-Sharing. A final, more contested concern was incomplete information-sharing among law enforcement authorities. While some interviewees thought information-sharing had greatly improved since 9/11, others expressed concern that the timely dissemination of information to local stakeholders remains a problem. Given the classified nature of some security threats, local police often have access to an incomplete or delayed assessment of a problem. This raises two vulnerabilities to a security threat. First, incomplete information can impede response times. A known phenomenon in cognitive psychology is the need for cognitive closure.[239] This problem means that when security officers face a large amount of uncertainty or missing information about a potential security threat, there is a tendency to discount the threat as `unlikely' to happen. This phenomenon can inadvertently blind security officers to an emerging threat and delay a necessary response.

Second, incomplete information can engender a false schema about the most likely types of threats and risk indicators to look for.[240] This is sometimes known as the idea that "generals tend to fight the last war." In the absence of information, security officers may defer to their understanding of "conventional terrorist threats," like the large-scale 9/11 attacks or *USS Cole* incidents. This concept, known as the availability heuristic, can blind law enforcement to more subtle ways in which NSAs may pose a threat, such as acting through the cyber domain. Further, "the absence of effective information and intelligence-sharing amongst security officials creates perceptions of exclusion and be a factor or barrier to the implementation of security measures at seaports."[241] This can contribute to low morale and hamper efforts to build resilience.

---

[237] Robert Bailey. "Rapid, Smart, and Flexible Acquisition." Ideas and Issues (Acquisition). Marine Corps Gazette. 2020. https://mca-marines.org/wp-content/uploads/Rapid-Smart-and-Flexible-Acquisition.pdf

[238] T.X. Hammes. "Technology Converges; Non-State Actors Benefit." Hoover Institution. February 25, 2019. https://www.hoover.org/research/technology-converges-non-state-actors-benefit; Andrew Philip Hunter. "The Change We Need: Making Defense More Future Proof through Adaptable Systems." CSIS. March 12, 2019. https://www.csis.org/analysis/change-we-need-making-defense-more-future-proof-through-adaptable-systems

[239] Donna M. Webster and Arie W. Kruglanski. "Individual differences in need for cognitive closure." Journal of personality and social psychology 67, no. 6 (1994): 1049.

[240] Yarin Eski. "The War on Meaninglessness: A Counter-Terrorist Self through an Absent Terrorist Other." *Ethnography* 17, no. 4 (December 2016): 460–79. https://doi.org/10.1177/1466138116639984.

[241] Eric L. Hampton. "Transnational Threats to Maritime Systems and Seaport Security." PhD Dissertation. Walden University. 2021. p. 42. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=11702&context=dissertations

Emerging Risks in the Maritime Domain

This section explains how these emerging threats and vulnerabilities interact to create several new security challenges for the MTS. These security risks differ from early maritime incidents in both their probability of occurrence as well as the scale of their impact. Addressing these emerging risks will require building on the MTSA and SAFE Port Acts and implementing new resilience-building strategies.

The central challenge to the effectiveness of the laws, regulations, and frameworks implemented in the wake of 9/11 is that the complexity of the current threat environment is outpacing maritime defense and response capabilities. First, the types of threats are changing. Rather than "high-impact" or "mega-terrorism" maritime incidents that some predicted following 9/11, the physical threat of violence in the maritime domain turned out to be more elusive. In particular, violent non-state actors have not only carried out maritime terrorism but have exploited the maritime environment for other operational and financial activities. The various activities that violent non-state actors conduct throughout the maritime environment create a more divergent threat environment than simply maritime terrorism.

Second, as several interviewees noted, the potential of some type of threat to manifest into a physical attack has increased. The complexity of the global MTS is creating new vulnerabilities by deepening the integration and co-dependence of ports and their operations. While a Mumbai-style attack is unlikely to occur, smaller events are more prevalent. The increasing reliance on maritime trade means that there is more traffic and larger vessels at sea, which arrive at ever busier and more automated ports. At the same time, states are likely to reorient their navies to a conventional force structure, investing in submarines rather than small boat patrols, for example, as global geopolitical tensions escalate. These economic and security trajectories create more entry points and areas of vulnerability for opportunistic and violent NSAs who have adapted, learned, and emulated others within this environment. As one interviewee stated, actors can maneuver with flexibility in this complex environment because they are "unencumbered by bureaucracy and resource acquisition."

Finally, there is now a more diverse range of actors who do not fit neatly with the terrorism-centric nature of existing regulations. For example, perpetrators of cyber-attacks in the maritime domain include transnational criminal organizations, hacktivists, state actors, "script kiddies," and insider threats, alongside traditional terrorists. Interviewees stressed the "blurry lines" between and within these actors. For example, non-state actors also commonly conduct attacks with the support of nation-states, making attribution and accountability more challenging. Within the criminal sphere, transnational organizations have acquired the skillset to smuggle drugs but are adopting new technology to facilitate other illicit activities like human trafficking. Moreover, homegrown violent extremists are an emerging threat without precedent within the maritime security space. These versatile and increasingly sophisticated foreign and domestic threats challenge conventional counter-terrorism risk management approaches.

Shifting Threat Environment

The changing landscape presents a number of new security challenges for maritime security stakeholders. We identify at least five emerging challenges to the MTS.

1. **New Domains for Exploitation**: The preeminent security challenge is the cross-cutting influence of other domains on the maritime space. The cyber domain presents a major change in how practitioners conventionally think about when and where security risks are most likely to materialize because they are no longer restricted to the physical domain. Instead, cyber risks present new tools, techniques, and opportunities to disrupt and degrade the MTS. Because cyber-attacks incur relatively few costs to implement and their effects are often hard to detect, their risk calculus is dramatically different than

conventional physical threats to the maritime arena. The cyber domain increases the likelihood of attacks with small, physical consequences but a high probability of success.

2. **Big Data and Information Processing:** A second major challenge for stakeholders is big data and information processing. Navigating the modern threat environment effectively requires identifying key warning signs and risk indicators within a dynamic and rapidly changing risk environment. However, increasing vessel traffic and the associated data output, the growing role of small actors below the nation-state threshold, and the rising number of MTS stakeholders lead to an increasingly complicated threat environment. Existing investigation and law enforcement resources cannot compile, organize, and analyze the massive amounts of data and information they receive. The strain on processing data could increase the likelihood of an attack materializing since necessary deterrence measures have not yet been determined.

3. **Attribution Challenges:** A similar major security challenge for stakeholders is ascertaining the perpetrator behind an attack. Since more actors now operate in the maritime domain, the number of potential non-state actors who could conduct an attack has exploded. This can make it increasingly hard and trace suspicious activities to specific actors. Similarly, since cyber and other new domains for exploitation are "grey-zone" activities, there is a growing attribution challenge. State actors may delegate attacks to non-state actors, creating new problems with plausible deniability and source attribution. This has consequences for both domestic and international security because it is more difficult to discern the scale of a threat, the probability it will occur, and the consequences it may have.

4. **Technological Innovation and Adaptation**: New information and communication technologies create both new threats (e.g. cyber, UAS, emerging weapons) and new vulnerabilities. A key challenge in combating these threats and vulnerabilities is maintaining a competitive edge. Adversaries tend to adapt to technological changes rapidly to maintain an edge in the threat environment. Slow resource acquisition times and delayed adoption of technological innovations can make it harder to deter or defend against these more recent threats. It can also make systems continuously vulnerable despite best efforts. A major challenge is that technology often puts stakeholders in a defensive position where they can react to emerging threats but can rarely pre-empt them.

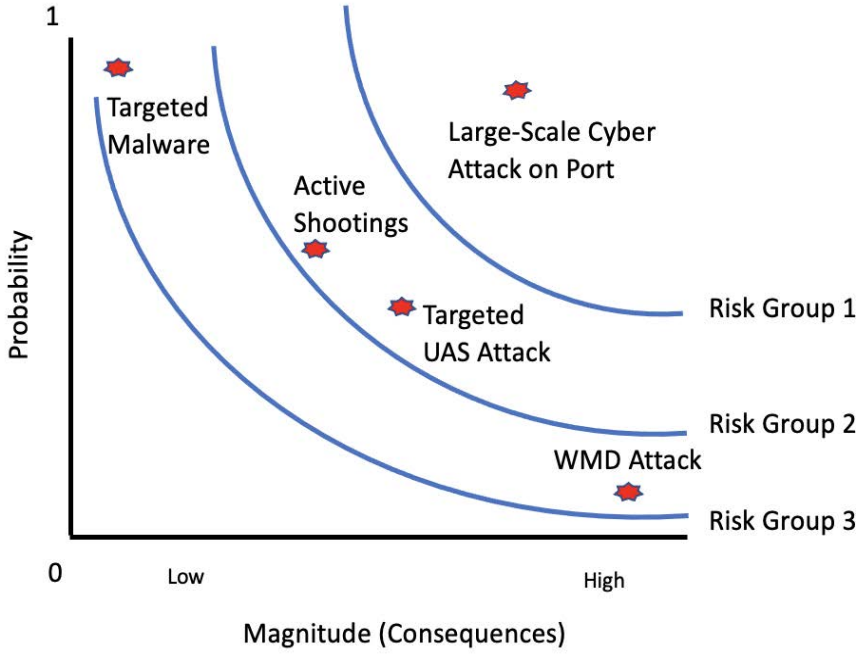
5. **Globalization and Increased Interdependence:** Globalization has created a more economically integrated and interconnected system. This not only links states closer together, but also means ports are increasingly reliant on single nodes—such as a common IT network system, natural chokepoint, or prominent shipping company—to facilitate the shipment of goods. When one of these nodes goes down, it may have cascading effects throughout the MTS. That is, an emerging security challenge is that the consequences of a maritime attack are no longer isolated to a particular port, vessel, or company, but can diffuse. An attack may have second-order or unintended consequences of other aspects of the MTS that can be hard to anticipate and avoid.

Risk Management and Assessment

Given these five challenges, we assess that the greatest threats to the MTS in 2021 are fundamentally different than threats to port security in 2001. The combination of an increasingly diverse threat environment along with a more numerous set of vulnerabilities across ships, ports, and people result in a different set of risks. This section analyzes these risks using the MSRAM equation: risk = threat x vulnerability x consequence.
We conceptualize different types of risks to the MTS based on their projected probability of occurrence and magnitude of effect (Figure 3). Probability describes the likelihood that an attack will have a non-zero impact or consequence on its intended target. A low probability attack is one that occurs infrequently, such as a 9/11-style physical attack. In contrast, a high probability attack may occur more routinely, such as a phishing attack or unauthorized access into a port. Magnitude describes the size of an attack's consequences on an intended target.

A low magnitude attack is one that incurs limited or minor damage on an intended target. A high magnitude attack has a broad and far-reaching effect on its intended target.

Figure 3. Assessment of Emerging Maritime Risks



This risk assessment framework builds on LCDR Brady Downs and Gary Gordon's MSRAM risk assessment framework.[242] Under this conceptualization, the most serious maritime risks are those with high probability and high magnitude (Risk Group 1). We categorize large-scale cyber-attacks on ports, similar to the cyber-attack on the Ukraine power grid, which have the potential to close a port for several days, as one of the most significant risks. Risk Group 2 encompasses scenarios that may occur with moderately high levels of probability and moderate consequences. For example, this can capture natural disasters such as a hurricane or earthquake, which closes a port for several hours. It can also include active shooter incidents or targeted UAS attacks against a vessel or port. Risk Group 3 encompasses *asymmetric* risks. These are risks which may have either a high probability of occurrence or a high consequence on an intended target, but rarely result in both. These asymmetric risks include not only large-scale physical attacks like the September 11 attacks or a potential WMD attack, but also small-scale cyber-attacks.

Practitioners have historically tended to prioritize high magnitude over high probability events, such as an attack using WMDs. After September 11, practitioners redirected their attention to risks that could portend another large-scale but low probability incident. While there remains a non-zero likelihood these can occur, extant initiatives have gone far in addressing this threat. Initiatives like the MTSA, SAFE Port Act, C-TPAT, and TWIC authorization program all aimed to minimize the likelihood of WMD smuggling inside the US or a 9/11-style attack in the maritime domain. The DHS took these actions based on the credible fear that if an attack

[242] Downs, Brady. Maritime Security Risk Analysis Model (MSRAM): "Balancing Resources to Risk." A presentation for the Critical Infrastructure Protection (CIP) Metrics and Tools Conference, June 2008; Gary Gordon. "Maritime Security Risk Analysis Model USCG Presentation to Area Maritime Security Committee." n.d. University of Massachusetts Lowell. https://faculty.uml.edu//gary_gordon/Teaching/documents/MSRAMPresentation.pdf

succeeded, it could have a broad impact on society. In sum, these security measures have helped constrain the risks of large-scale, but low probability incidents.

Due, in part, to the effectiveness of these programs, and the rapidly changing threat environment, our assessment of the greatest risks today is changing. While large-scale, low probability attacks guided risk management strategies after 2001, we assess the greatest risks today are small-scale, but high probability incidents. New tools, technologies, and non-state actors make it easier than ever to conduct an effective attack against the MTS. We present different scenarios which explain how and why these small-scale, low-probability attacks may occur.

Potential Risk Scenarios

A. Cyber-Attacks: Disruption, Distortion, and Deterioration

The emergence of the cyber domain has dramatically increased the risk of cyber-attacks against the MTS. We assess cyber-attacks to be emblematic of the high probability, but low consequence risks to port security.

Table 6. Characteristics of Cyber Risks in the Maritime Domain

Attack Variables	**Characteristics**
Perpetrators	• States • Transnational criminal organizations • Script kiddies • Hacktivists • Terrorist groups

Objectives	• Operational
	  ○ Collecting information and data
	  ○ Facilitate attacks and follow-on attacks
	  ○ Disrupt or delay operations
	• Financial
	  ○ Collecting ransom
	  ○ Trafficking goods or people
	  ○ Selling information and data
	• Strategic
	  ○ Deterrence
	  ○ Activism

Targets	• People
	  ○ Company
	  ○ Crews
	  ○ Operators
	• Infrastructure
	  ○ Ports
	  ○ Vessels
	  ○ Bridges
	• Goods
	  ○ Data
	  ○ Cargo

	○ Passengers
Target Systems	● Cargo systems ○ Cargo Manifest ○ Container controls ○ OCR cameras ● Security systems ○ Cameras ○ Firewalls ● Vessel Systems ○ Communications ○ Navigation ● Operational systems ○ Servers ○ Smart grids ○ firmware ○ Vessel Traffic Service ○ Voice Over Internet Protocol (VoIP)
Attack Vectors	● Phishing ● Spoofing ● Malware ● Ransomware ● Man-in-the-middle attack ● Denial of service
Example Incidents	● Maersk NotPetya attack, June 2017 ● CMA CGM attack, September 2020 ● Colonial Pipeline attack, May 2021

First, we assess the probability of a cyber-attack as higher today than a conventional physical attack because people may overestimate their ability to deter and detect a cyber-attack. IT departments are small and constrained by resources. Cyber hygiene standards are not mandated, so there are inconsistent levels of protection within a company, port, and vessel's security systems. Finally, companies have incentives not to disclose when they experience a cyber-attack, making it harder to identify the causes, impact, and future mitigation steps of an attack.

Second, the barriers to conducting a small cyber-attack are low. Although most attacks have limited damage, it is increasingly likely that we might see a large-scale cyber-attack due to an increasing amount of zero-day exploits. These are found on the dark web and are essentially ready-to-go malware for cyber- attacks. Stuxnet is probably one of the more famous examples of a zero-day exploit, but it refers to any piece of original, malicious

code for which there are no immediate patches available. It is very easy for an attacker to go on the dark web (e.g. Soup2Nuts), purchase an exploit, and deploy with relatively little technical expertise. Most likely, we would see this occur in the context of a denial of service attack (or botnet).

Despite the large number of vulnerabilities onboard ship systems, the risk of a cyber-attack against a vessel is likely to be of relatively low consequence. A key mitigating factor to the risks of cyberthreats and automated vessel systems is their containment potential. Unlike port systems which increasingly rely on hub and spoke models, vessel systems are relatively self-contained. As a result, malware or other cyber threats may not spread or have as far-reaching consequences as attacks directed at ports.

A key concern is the potential for a port-directed cyber-attack to grow into a large-scale incident (Risk Group 3 → Risk Group 1). This scenario could occur if a delayed response allows the cyber-attack to leverage hub and spoke network systems to grow and infect multiple systems. There is a higher likelihood of cascading effects because the increasingly interconnected network of systems makes it harder to anticipate the impact of an attack precisely. The nature of the maritime sector—being a "system of systems"—means that an attack in one system has a second-order effect on other, connected systems. The linkages between "multiple and diverse systems" within the maritime domain will continue to expand and increase through the Internet of Things and the use of 5G.[243] For example, the NotPetya attack on Maersk had an even larger effect than initially anticipated because the malware could spread across the computer network. The ransomware attack on the Colonial Pipeline did not have much success in delaying the transport of oil, but it had unexpected ramifications on consumer behavior, inducing a wave of panic-buying on news of an attack.

Although there is a non-zero change of a large-scale coordinated cyber-attack comparable to 9/11 or Mumbai, it would require a greater deal of sophistication and would likely occur in conjunction with a physical attack. For example, if a large container ship is attacked while traveling through a restricted navigation area in a major port, the vessel may lose power, steerage, or propulsion, and cause the vessel to run aground. This cyber-attack could manifest physically, as the vessel may block a strategic maritime gateway and potentially disrupt the global commerce flow for days.

Box 10. Cybersecurity and Smart Ports
Case Study: Port of Rotterdam
Europe's largest port is the Port of Rotterdam, a smart port that handled 436.8 million tons of cargo in 2020.[244] Rotterdam has maintained its competitive edge by leveraging automation, digitalization, and other technological advances within its logistics supply chain. The port models "smart logistics," which refers to the more efficient organization of physical logistics and information logistics in domestic and international transport chains and networks.[245] This approach integrates existing logistics technologies through innovations such as Big Data and the Internet of Things to improve the efficiency of logistics processes in real-time. Smart ports, such as Rotterdam, have adopted the "smart logistics" approach to meet the global demand for goods. However, the technologically advanced and networked systems also increase the exposure to and impact of cyber threats.

[243] Andrej Androjna, Tanja Brcko, Ivica Pavic, and Harm Greidanus. "Assessing Cyber Challenges of Maritime Navigation." *Journal of Marine Science and Engineering* 8, no. 10. October 3, 2020. p. 11. https://doi.org/10.3390/jmse8100776
[244] "Port of Rotterdam Facts and Figures." Port of Rotterdam Authority. https://www.portofrotterdam.com/sites/default/files/2021-06/facts-and-figures-port-of-rotterdam.pdf
[245] Sahbia Bessid, Ala Zouari, Ahmed Frikha, A. Benabdelhafid. "Smart Ports Design Features Analysis: A Systematic Literature Review." HAL Archive. November 2020. p. 3. https://hal.archives-ouvertes.fr/hal-03177580/document

Smart port terminals use industrial control systems that translate sensorial data and commands into mechanical actions.[246] However, the networks that link mechanical and sensorial systems provide abundant entry points for cybercriminals to conduct an attack. Furthermore, it is difficult to identify and fix bugs and weaknesses within an automated system because of the integrated nature of its components. Determining, identifying, addressing a vulnerability must also occur without compromising the transportation of cargo. Finally, without adequate data network monitoring and risk management systems in place, modern ships risk spreading cyber viruses onto port systems.

Additional cyber-related risks include overused and outdated group passwords, personal passwords shared between colleagues, and weak PINs shared on unsecured channels. In one survey, companies indicated that they use network segmentation for all or part of their IT environment, but simulated cyber-attacks demonstrated that separation had not been arranged properly at all locations.

For example, when the NotPetya brought down Maersk, Rotterdam's fully automated APM Terminal was also compromised.[247] APM handles a third of total traffic at Rotterdam's Maasvlakte harbor basin. If the other two terminals had been affected by the malware attack, there would have been massive economic losses. While the fully automated terminal was not operational until over a week after the attack, an older terminal was reopened after three days since it is not fully automated, meaning containers can be handled manually, and crane technology operates independently.

The Netherlands' Ministry of Economic Affairs and Climate Policy funded a report to raise cybersecurity awareness and provide tools to improve security against cybercrime.[248] Eight companies across the logistics supply chain participated through questionnaires, interviews, and simulation exercises. Nearly all of the companies reported cybercrime attempts, and one-fifth stated that a cyber incident temporarily shut down their business operations. The companies indicated that they had been targets of cyber-attacks aimed at specific functions, employees, and business units. Participants state that "the human factor" is a particular challenge, as companies view their employees as the most critical source of protection against cyber incidents while also considering them the greatest risk to digital security. While major incidents are an impetus for companies to refocus their efforts on cyber resilience, over time, employees' awareness of cyber hygiene and security processes wavers, and priorities shift to reactive measures.

Participants also noted that, in most cases, companies do not inform each other if a cyber incident has occurred or is occurring, do not discuss cybersecurity during supply chain meetings, and overall, do not share security policies and sensitive information. Additionally, more than a third of the logistics companies revealed that they do not have a crisis plan that can be activated in the case of a cyber incident. Furthermore, 40% of the crisis plans in place have never been tested, and employees are not aware of them.[249]

B. Extremist Violence: New Actors and New Opportunities

The number of international and homegrown extremist threats is growing. The threat of Al Qaeda has not entirely dissipated. Further, the addition of new domestic extremism threats, including eco-terrorists, hacktivists, and active shooters, raises the likelihood of a domestic attack. Given the broad number of potential

[246] Philipp Martin Dingeldey. "Port Automation and Cybersecurity Risks." Maritime Executive. December 22, 2017. https://www.maritime-executive.com/editorials/port-automation-and-cybersecurity-risks
[247] "Smart port in Rotterdam confounded by cyber-attack." Dutch News. June 30, 2017. https://www.dutchnews.nl/news/2017/06/smart-port-in-rotterdam-confounded-by-cyber-attack/
[248] Robin de Veer and Robert Wezeman. "Onderzoek Cybersecurity In De Logistieke Keten." TNO. December 11, 2020. https://smartport.nl/wp-content/uploads/2021/02/Onderzoek-Cybersecurity-in-de-Logistieke-Keten.pdf
[249] Ibid.

perpetrators, attacks may occur at foreign points, vessels en route, and domestic ports, increasing the potential number of targets law enforcement must protest. For these reasons, we again assess a higher probability of extremist violence even if current counterterrorism response capabilities mitigate the consequences of these attacks.

Table 7. Characteristics of International and Homegrown Extremist Attacks in the Maritime Domain

Attack Variables	Characteristics
Perpetrators	● Insider threats ● Active shooters ● Homegrown violent extremists ● Foreign terrorist organizations
Locations	● Concentrated shipping ports and lanes (Panama Canal, Suez Canal, Strait of Malacca) ● Major US ports (Port of LA, Port of Long Beach, Port of New York and New Jersey, Port of Savannah) ● Southeast Asia ● Middle East and North Africa ● Sub-Saharan Africa
Objectives	● Operational o Transporting recruits o Transporting goods o Threatened or actual attack on maritime target ● Financial o Taking resources (piracy, kidnapping for ransom, oil bunkering) o Trafficking of goods or people o Taxation and extortion ● Strategic o Intimidation (hijacking, indiscriminate violence) o Activism o Recruitment
Targets	● Passenger cruise ships and ferries ● Cargo vessels ● Oil tankers ● Oil and glass platforms
Attack Vectors	● Firearms ● Explosive devices ● Mines and maritime IEDS ● Small boats (suicide boats and drone boats) ● Unmanned, underwater vehicles
Example Incidents	● Eduardo Moreno, USNS *Mercy*, Port of Los Angeles, April 2020 ● Aaron Alexis. Naval Sea Systems Command, Washington Navy Yard, September 2013 ● Abu Sayyaf Group (ASG), *Superferry14,* Manila, February 2004 ● Lashkar-e-Tayyiba, Mumbai, November 2011

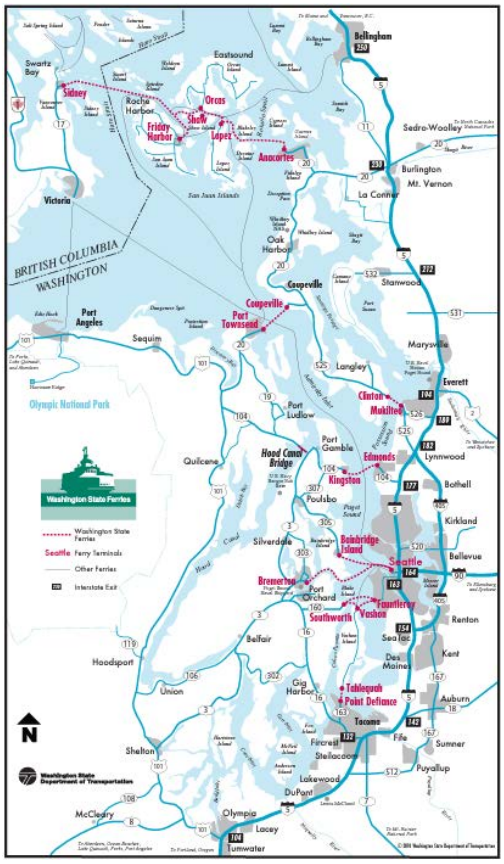
Historically, notable mitigating factors of extremist attacks in the maritime domain were (1) the operational difficulties of conducting an attack at sea and (2) the limited visibility of an attack. These conditions were thought to constrain both an extremist group's motive and capacity to carry out an attack. These mitigating factors have two key implications. First, high operational barriers imply that the risk of violent non-state actors carrying out physical attacks in the maritime domain is related to the potential target's level of vulnerability to the potential attacker's tactics and weapons. Rather than preparing for limitless maritime attack scenarios, potential targets should develop defensive capabilities and establish contingency plans that violent NSAs are likely to exploit. One interviewee also emphasized considering maritime geography when developing strategies to intercept violent NSA operations. For example, one potential risk indicator related to maritime geography is informal landing sites along coasts, particularly when the unloading capacity of the formal port is limited. If these vulnerability indicators are addressed, conducting a maritime attack will have limited strategic utility for violent NSAs.

Still, the growing number of opportunities to interfere with vessels both en route as well as at ports can reduce some of the operational barriers to staging attacks. There are increasing blind spots that an actor can exploit—whether it is weakening physical security, poor cyber defenses, or growing container traffic—to achieve their objectives. Similarly, emerging technologies such as UASs, the Internet, and other new information technologies (e.g. cell phones) can make it easier for extremists to advertise their attacks.

Second, if an attack aims to intimidate, advertise, or draw attention to a group's goal, then conducting it offshore would not illicit the same response as an attack on land. However, this also means that violent NSAs use the maritime domain for other activities beyond being a vector of attack. A Stable Seas report illustrates that sea blindness—the tendency for states to ignore the maritime environment—has allowed violent NSAs to manipulate and exploit it, even when their ability to conduct physical attacks fluctuates.[250] Stable Seas' Megan Curran describes five specific activities violent NSAs operating in the maritime space engage in.[251] Operationally motivated activities include tactical support—specifically on-land raids by sea and the movement of fighters via sea routes—and conducting maritime attacks, including cyber-attacks, against maritime targets. Financially motivated activities include taking, trafficking, and taxing and extorting. The "taking" activities include oil bunkering, kidnapping for ransom, and piracy. Trafficking activities include drug trafficking, migrant smuggling, and money laundering. This Stable Seas framework highlights the range of activities undertaken by violent NSAs within the maritime domain. Therefore, potential targets and stakeholders must identify the specific environmental risk factors that would make them vulnerable to one or several of these illicit maritime activities and develop strategies to mitigate them.[252] Extremists derive utility out of operating in the maritime space independent of the strategic logic of advertising. This means extremists today have alternative incentives to operate in the maritime domain, raising the likelihood of an attack.

[250] Meghan Curran. "Soft Targets & Black Markets: Terrorist Activities in the Maritime Domain." *Stable Seas.* May 2019. p .11. https://www.stableseas.org/post/new-report-terrorist-activities-in-the-maritime-domain
[251] Ibid.
[252] Ibid, p. 27

Box 11. Risk of Terrorism and Violent Extremism on Passenger Ferries
Case Study: The Washington Ferry System



Washington State has the most extensive ferry system in the United States. It includes 21 auto-passenger vessels, 20 terminals on ten routes, and about 2,000 employees.[253] The functions of the Washington State Ferry System include linking the region's multimodal connections, moving freight and goods, and tourism. The ferry system also expects a ridership growth of 30% over the next 20 years. However, operating increasingly high-capacity passenger vessels also represents a possible target for terrorism or violent extremist attacks, including hijacking, littoral attacks, and explosive devices.

Ferries within the Washington Ferry System are in service 20+ hours a day. During this time, vessels are expected to transport high volumes of traffic within a specific schedule. Efficiency may be a tradeoff for security, as haphazard or brief security checks make it easier for potential attackers to smuggle firearms or other weapons aboard.

Another vulnerability is that, as a hub of regional travel, the Washington State Ferries schedule information is publicly available online for each route.[254] The website also has details about the vessels in its fleet, including the year built, size, speed, passenger amount, and class.[255] Having these fixed schedules and transparent vessel information lowers the threshold of knowledge needed to plan and conduct an attack.

Finally, the Washington Ferry System, with 21 vessels, has an aging fleet "with all but 12 vessels over 30 years old."[256] This not only means that vessels may lack advanced operating systems, but that the integrity of their existing structure may be more vulnerable to being compromised. Moreover, when a vessel does break down, there is only one relief boat, and drydock capacity in Puget Sound is limited, making it difficult to adapt to emergency repair situations. Despite maritime passenger vessels accounting for only a sliver of the U.S. commercial transportation industry, they are attractive targets for violent extremists whose objectives include inflicting mass human casualties.

While maritime law enforcement has implemented robust capabilities to detect nuclear explosive devices and radiological disposal devices, less attention has focused on how existing vulnerabilities could enable a more conventional attack, such as a maritime improvised explosive device (MIED) attack or an active shooter incident. This omission is significant given the high probability that a conventional attack could destabilize the MTS. For example, researchers simulated an MIED attack on

[253] "Washington State Ferries." WSDOT. January 2021. https://wsdot.wa.gov/sites/default/files/2020/09/15/WSF-FactSheet-January2021.pdf
[254] See https://www.wsdot.com/ferries/schedule/
[255] See https://wsdot.wa.gov/ferries/terminals/our-fleet
[256] "Washington State Ferries." WSDOT. January 2021. https://wsdot.wa.gov/sites/default/files/2020/09/15/WSF-FactSheet-January2021.pdf

the Seattle Passenger Ferry System and the MTS in Puget Sound, Washington.[257] In this scenario, attackers successfully planted and detonated MIEDs on a ferry, causing 200 casualties, and coordinated a second attack on a cargo vessel, rendering it immobile. The exercise analyzed the responses of military, law enforcement, and civilian agencies to the crisis scenario. In the simulation, the response groups evacuated all dead and injured personnel from the ferry in 16 hours. In reality, due to operational capacity limitations, this would have taken much longer. Moreover, the time needed for the appropriate teams to arrive and neutralize the MIEDs would have taken longer in real-time, compared to the wargaming results. This exercise highlighted which challenges need to be addressed to quickly mobilize first responders following an attack and the potential future force structures to streamline port security.

In 2017, a first-ever joint agency exercise simulated an active shooter incident aboard the Washington State Ferry's new vessel, *Chimacum*.[258] Participants included Coast Guard Sector Puget Sound, Customs and Border Protection, Washington State Ferry, Washington State Patrol, King County Sheriff's Office, and Everett Police Department. This exercise provided insight into how passengers would react to an active shooter event and how quickly law enforcement personnel would respond. Though this was a useful exercise, it also revealed that a large number of casualties would result from an armed passenger open firing on a ferry and that law enforcement would likely have a delayed response to such an event.[259] Local law enforcement and security partners need to continue training exercises and share best practices to improve their response time and coordinate in the event of an attack. As one participant stressed after the exercise, "we need to be situationally aware at all times… don't fall into routine, and don't become complacent."[260]

C. Advanced Technology Systems: New Tools, Tactics, and Risk Magnifiers

In addition to the threats posed by cyber-attacks and extremist actors, we assess the advent of new and sophisticated technology systems as a growing risk. Advanced technology systems heighten the probability that threats materialize because they provide non-state actors new tools and tactics to execute these attacks. At the same time, these technology systems are not yet advanced enough to result in large-scale physical damage the same way as a conventional explosive or WMD attack.

Emerging advanced technology systems are a risk magnifier in today's environment because they heighten the probability an attack succeeds. The ability of a NSA to adopt and leverage advanced technologies – coupled with slow response times and adaptation challenges—makes it more difficult for law enforcement to deter and detect threats. Adversaries tend to adapt to technological changes rapidly to maintain an edge in the threat environment. For example, a common cyber hygiene practice to minimize the risk of cyber-attacks is patching and routing updates, which often come out on Tuesday. In the cyber realm, many NSAs leverage "patch Tuesday, hack Wednesday" to describe how they spend the day after the patches come out to break down how they operate.[261] These allow non-state actors to then issue new threats rapidly. Slow resource acquisition times and delayed adoption of technological innovations can make it harder to deter or defend against these more

[257] Richard Jimenez, Bobby Rowden, Eugene Paulo. "Using System Simulation and Wargaming to Examine The Threat of Maritime Improvised Explosive Devices (MIEDs) In U.S. Ports." Calhoun Institutional Archive of the Naval Post Graduate School. 2006. https://calhoun.nps.edu/bitstream/handle/10945/45707/Paulo_GCMS_MIED_Wargame_paper_final_2009-07.pdf?sequence=1&isAllowed=y

[258] Thomas Bliss. "Vessel Safety, Security & Response to Hostile Actors." The Northwest Marine Academy. May 24, 2017. https://northwestmaritimeacademy.com/vessel-safety-security-response-hostile-actors/

[259] Steven A. Blindbury. "Safe Seas: Protecting America's Ferries Against Criminal Mass-casualty Incidents." Journal of the NPS Center for Homeland Defense and Security 17. December 2018. p. 8. https://www.hsaj.org/articles/14937

[260] Thomas Bliss. "Vessel Safety, Security & Response to Hostile Actors." The Northwest Marine Academy. May 24, 2017. https://northwestmaritimeacademy.com/vessel-safety-security-response-hostile-actors/

[261] "Patch Tuesday, Exploit Wednesday, and Zero-Day Attacks." Safety Bytes. 2016. https://safebytes.com/patch-tuesday-exploit-wednesday-and-zero-day-attacks/

recent threats. It can also make systems continuously vulnerable despite best efforts. A major challenge is that technology often puts stakeholders in a defensive position where they can react to emerging threats but can rarely pre-empt them.

Table 8. Characteristics of Emerging Technology Attacks in the Maritime Domain

Attack Variables	Characteristics
Perpetrators	● Revisionist States ● State-sponsored actors ● Foreign terrorist organizations ● Transnational criminal organizations ● Homegrown violent extremists
Locations	● Active war zones/insurgencies (e.g. Yemen, ISIS) ● Gray-Zone Conflict/Frozen Conflict (e.g. Ukraine, Azerbaijan) ● Shipping routes/natural chokepoints (e.g. Bab-el-Mandeb) ● Urban areas ● Major U.S. ports

Objectives	● Operational
	  ○ Intelligence, surveillance, and reconnaissance
	  ○ Improve command and control
	  ○ Target acquisition
	  ○ Threatened or actual attack
	● Financial
	  ○ Trafficking of goods and people
	● Strategic
	  ○ Recruitment
	  ○ Propaganda

Targets	● Military Targets
	  ○ Infrastructure
	  ○ Personnel
	● Maritime Vessels and infrastructure
	  ○ Passenger cruise ships and ferries
	  ○ Cargo vessels
	  ○ Fuel tankers
	  ○ Undersea telecommunication cables
	  ○ Oil and natural gas platforms
	  ○ Transportation routes and vehicles
	● Civilian Locations
	  ○ Schools
	  ○ Hospitals
	  ○ Homes
	  ○ Commercial planes

Attack Vectors	● Lethal autonomous weapons systems
	● Unmanned aircraft systems (UASs)
	  ○ Commercial UASs
	  ○ Military-grade UASs

	• Unmanned surface vehicles
Attack Examples	• Houthi USV attack on BW *Rhine* oil tanker, Saudi Arabia, December 2020 • Iran-back UAS attack on oil tanker, Oman, August 2021

One of the major concerns is that new types of threats can interact with each other to amplify the risk of an incident. NSAs may incorporate emerging technologies and cyber tools into existing capabilities to stage attacks. The use of UAS by NSAs like ISIS demonstrates its relative ease of adoption (Box 2). These technologies require little expertise to operate and therefore can be manipulated by small non-state actors to carry out attacks. In conjunction with the growing swath of NSAs intent on carrying out violence against maritime targets, advanced technology systems have the potential to raise the risk of an attack.

Box 12. Potential for Escalatory Attack Vectors
Case Study: Port of Houston

One interviewee from the Port of Houston argued that maritime security forces need to frame threats such as unmanned aerial vehicles, environmental terrorism, cyber-attacks not as threats themselves, but as attack vectors. These vectors increase the risk of TSIs by creating more opportunities and tools to conduct attacks. The interviewee emphasized that identifying attack vectors and their potential role in a TSI is necessary for improving prevention measures. Reviewing the recent disruptions the Port of Houston has experienced is helpful in understanding the range of attack vectors a single maritime target could face in a TSI. Located in the fourth-largest city in the United States, the Port of Houston is the number one US port in foreign waterborne tonnage and number three US port in terms of total foreign cargo value.[262]

In April 2018, a small camera equipped UAS, fell out of the sky, trailing smoke over the Port of Houston's Turning Basin Terminal.[263] Prior to its crash, the UAS flew around the port for at least 30 minutes, taking over 60 photos of vessels, rail infrastructure, and other structures. Within minutes of the incident, port police and firefighters arrived to intercept the UAS. The Federal Aviation Administration requires hobbyist UAS operators to contact air traffic control and/or airport management if they are operating within a 5-mile radius of any local airport, which includes the Turning Basin Terminal given its proximity to Hobby Airport. While an investigation revealed that a freelance photographer was using the UAS, the incident underscored significant security gaps regarding UASs. Interviewees stressed that ports do not have the capability to shut UASs down; they can only intercept the UAS if it lands and report the incident. This event exposed the potential for a commercial UAS to be used as an attack vector, including surveillance, coordinating an attack, and carrying an explosive payload.

Another disruption that the Port of Houston has experienced is environmental activism. On September 12, 2019, a group of Greenpeace USA climate activists rappelled off a bridge, causing a part of the Houston Ship Channel to shut down for about 18 hours.[264] The activists were protesting the use of fossil fuels ahead of the Democratic primary debate that was taking place that evening in Houston. The Port of Houston, located along the channel, was targeted since it is home to the largest petrochemical

[262] "Statistics." Port Houston Trade Development Information. https://porthouston.com/about-us/statistics/
[263] "Increased Use of Drones Raises Security Concerns." Port of Houston Navigator. Summer 2018. p. 19. https://portarchive.com/2018/PH-Navigator-SUMMER-2018.pdf
[264] Morgan Gstalter. "Greenpeace activists rappel off Houston bridge to protest fossil fuels before Democratic debate." *The Hill*. September 12, 2019. https://thehill.com/homenews/campaign/461119-greenpeace-activists-rappel-off-houston-bridge-to-protest-fossil-fuels

complex in the United States. In addition to two lanes of traffic on State Highway 146 being closed on the bridge, the incident also disrupted the flow of vessel traffic moving through the channel. While this protest did not escalate to eco-terrorism, it highlighted the determination of activists to garner media attention to bring attention to their cause and the possibility of violent attackers to target junctures of critical infrastructure. Recently, a report by the Houston Health Department and One Breath Partnership found that high concentrations of formaldehyde—a cancer-causing chemical—were detected in Houston neighborhoods near the port's petrochemical complex.[265] Specific port operations, such as those that raise environmental and health concerns, could become motivating factors for future disruptions and attacks.

Recently, two container terminals in the Port of Houston were shut down because of a hardware failure. According to a letter from the port's executive director, the storage devices that support the applications to operate the Barbours Cut and Bayport Container Terminals failed.[266] Staff responded by moving the applications and associated data to redundant storage devices, which also failed a few hours later. The terminals, which handle about two-thirds of all the containerized cargo in the Gulf of Mexico, could not process incoming vessels and operate truck gates.[267] Although this was not a cyber-attack, the fact that both the initial hardware and their redundant systems failed revealed a critical vulnerability to the port's operation. Non-state actors like script kiddies could exploit this type of vulnerability to breach a maritime computer system and perform internal reconnaissance on the integrity of hardware systems before determining an appropriate attack vector. These three excerpts on recent disruptions at the Port of Houston highlight the potential for a wide range of escalatory attacks on critical infrastructure.

Resilience-Building and Mitigation Strategies

Given the risks in today's threat environment, we anticipate a higher likelihood of non-state actors trying to infiltrate, disrupt, and degrade the MTS. To address these risks, practitioners may consider investing in three strategies:

1. **Deter:** These deterrence strategies aim to reduce the probability that an attack occurs. This may take the form of target hardening or cyber-hygiene. The end goal is to improve resilience and limit vulnerabilities to an attack.

2. **Detect:** These prevention strategies aim to reduce both the probability and consequences of an attack by identifying emerging threats, detecting anomalies, and taking pre-emptive steps to reduce their likelihood. The end goal is to disrupt threats before they materialize.

3. **Deliver:** These mitigation strategies aim to reduce the consequences of an attack. The end goal is to react to incidents after they occur with a timely and effective coordinated response.

[265] "Formaldehyde Air Pollution In Houston." Environmental Integrity Project. July 1, 2021. https://environmentalintegrity.org/reports/formaldehyde-air-pollution-in-houston/
[266] Roger Guenther. "Port Houston" July 28, 2021. https://porthouston.com/wp-content/uploads/Letter-to-Industry-Jul-2021.pdf
[267] Mike Schuler. "Port of Houston Container Terminals Shut Due to 'Hardware Failure.'" Captain. July 28, 2021. https://gcaptain.com/port-of-houston-container-terminals-shut-due-to-hardware-failure/

Figure 4. Resilience-Building Steps for Emerging Maritime Risks

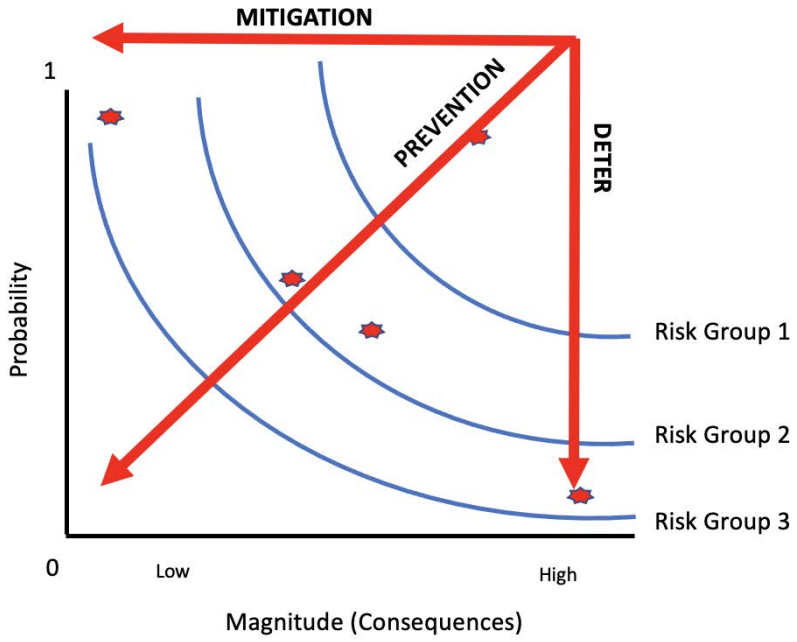


Figure 4 illustrates how each of these strategies can reduce the risk of an attack against the MTS. While these strategies can often mitigate or constrain the consequences of an attack, it is impossible to eliminate these risks. NSAs adapt and innovate in response to counterterrorism practices. The effectiveness of post-9/11 measures is part of the reason why non-state actors changed the tactics and tools used to carry out their attacks. Nevertheless, we believe that building on the MTSA and innovating new strategies can effectively confront the present risks in today's threat environment. Future research should continue to evaluate how the risk environment is changing in order to stay ahead of the curve and counter-adapt to non-state actor innovations.

Based on recommendations and examples from interviews, we focus on five areas where practitioners can mitigate these risks and improve resilience against a potential attack. These areas include:

1. Machine Learning
2. Personnel Training and Operational Exercises
3. Wargaming and Simulation Exercises
4. Regulations
5. Reflections and Lessons Learned

For each area, we describe how these strategies can mitigate risks. We also provide examples and potential applications of how the maritime domain can adopt these recommendations.

Machine Learning

Big data and information-processing challenges can make effective counterterrorism and defense operations harder to achieve. However, big data and technological innovations can also be a boon to improve counterterrorism and defense operations. These techniques may leverage Machine Learning (ML) or artificial intelligence to improve detection efforts and improve responses. ML is a form of artificial intelligence increasingly used in computer science and social science to solve complex prediction problems. It involves a set of computer algorithms that learn patterns in existing or historical data and extrapolate predictions based on this

information. ML is already applied in other sectors of defense operations to assess international security threats. Integrating ML algorithms into existing USCG, CBP, and DHS risk assessments can allow for analysis of more fine-grained data on domestic and transnational terrorist threats.

There are three advantages to incorporating ML into risk assessment frameworks moving forward:

- ML provides a generalizable framework to assess different terrorist threats. Its main performance metric is centered around predicting out-of-sample cases. We can input data about emerging threats and extrapolate how serious a threat it is. This means it can be useful to interpret a wildly changing or unpredictable environment.
- ML quickly detects patterns in large amounts of information to assess what warning signs are most important.
- ML identifies the most relevant risk indicators from across a wide array of information. It does not make any assumptions about what information is important to understand a particular outcome. This means we can input many potential risk indicators into ML models without worrying about overlooking key indicators.

Overall, ML has the potential to improve detection and response capabilities. Because it can sort through large amounts of information quickly, it can better assess where vulnerabilities may arise, what types of threats are likely to materialize, and how practitioners can better prioritize resources across a large set of targets to best mitigate the risks. This means it can address emerging challenges related to information processing, attribution challenges, and technological innovation. Potential machine learning applications include:

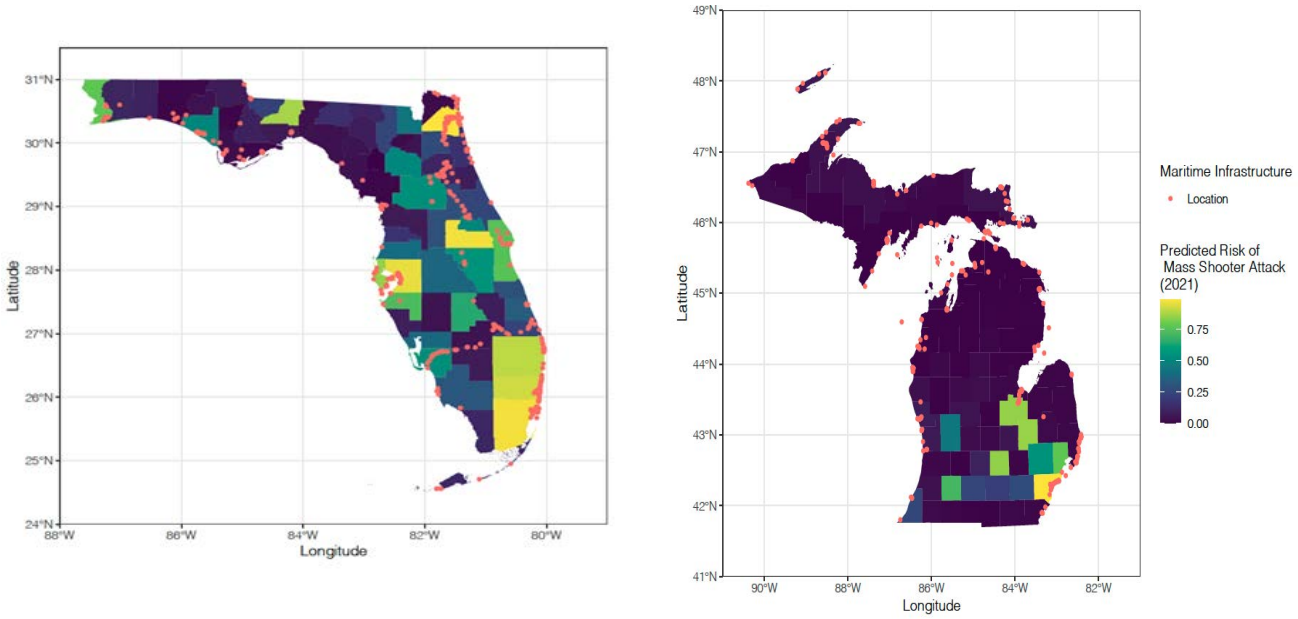
1. **Deter:** Vulnerability Mitigation
2. **Detect:** Anomaly Detection, Threat Assessment
3. **Deliver:** Target Attribution, Resilience-Building

Vulnerability Mitigation. ML for vulnerability planning could help law enforcement identify areas most at risk for violent attacks, piracy, unauthorized port entry, or other types of interference. As the threat landscape becomes more complex, machine learning can help identify which areas are most vulnerable and help practitioners optimize resource allocation to secure these areas. This research would use geospatial information about routes, port layouts, or navigable rivers and waterways. It could then use historical data about pirate attacks, terrorist attacks, lock failures, or unauthorized port entries to determine where these incidents are most likely to occur.[268]

Example: A team at the University of Southern California Center for Artificial Intelligence maps critical infrastructure for the City of Los Angeles in order to determine where earthquake-resilient pipes are most needed.[269] Malone and Strouboulis (2021) use information on the location of USCG-affiliated ports and waterways to identify which areas are most at risk for an active shooter incident.[270] Using historical information on active shooter incidents, they build a basic classification model that predicts with 91% accuracy where an active shooter incident is most likely to occur inside the United States.

[268] Similar efforts could use "Spyglass" to anticipate illegal fishing activity. This open-source resource provides information on vessel crimes. This could be paired with geospatial information to anticipate where illegal activities is most likely to take place and then take steps to intercept or deter such events. (See: https://spyglass.fish/)
[269] Gary Polakovic. "The next big effort in AI: keeping L.A.'s water flowing post-earthquake." USC. 2019. https://news.usc.edu/160680/ai-la-water-supply-earthquake-usc-research/
[270] Iris Malone and Anastasia Strouboulis. "Predicting Domestic Extremism and Targeted Violence: A Machine Learning Approach." June 2021. NCITE: Omaha, NE.

Figure 5. Predicted Risk of Active Shooting Incidents and Proximity to Maritime Infrastructure in Florida and Michigan (Malone and Strouboulis 2021)



Anomaly Detection. Anomaly detection is another ML application which can improve detection capabilities. Anomaly detection is a type of unsupervised machine learning approach. This method traditionally describes patterns in large amounts of data by classifying similar observations into distinct "clusters" or "classes." Anomaly detection could bolster counter-terrorism, counter-drug, and counter-trafficking efforts. Interviewees noted, for example, that small vessel traffic within ports can be concerning because it is unclear whether the traffic is nominal or not. Machine learning can learn patterns associated with nominal traffic. It could then read real-time information to ascertain and classify whether vessel traffic is consistent with this activity. If it falls outside the bounds, then traffic may be prioritized for inspection.

Similar processes could be used to examine AIS traffic to determine whether vessels are taking longer than expected to arrive at a port or are taking unusual routes. Investigators could use open-source data from *MarineTraffic* to build a real-time ML model to detect anomalous shipping traffic. Efforts like these are already under development through the CCRi port-based anomaly initiative, which scores the risk level of incoming traffic based on their routes.[271]

Example: A key concern from interviews is data manipulation of cargo manifests. Machine learning can assist in identifying "anomalous" cargo by looking for inconsistencies between cargo manifests and physical information about a given container.

As a proof-of-concept exercise, we collected a random sample of container manifests shipped between December 2020-February 2021 from *ImportYeti*.[272] This open-source website provides bill of lading information from U.S. Customs Sea Shipment Records. This information is free and available for download. We apply an unsupervised machine learning density-based clustering algorithm to a random sample of 28,434 containers. This algorithm looks for anomalous containers based on four inputs: container weight, TEU, quantity, and Harmonized System (HS) Code. The algorithm sorts and classifies different containers based on similarities in these inputs. For example, containers carrying concrete have a particular HS code and also tend to

[271] Nallon, Eric. "Detecting Anomalous Vessels at Maritime Ports." General Atomics CCRi. 2021. https://ccri.com/detecting-anomalous-vessels-at-maritime-ports/
[272] See https://www.importyeti.com/

have higher container weights than containers carrying cotton or wool. The analysis flagged 46 containers (0.16%) as anomalous. This means these containers had weights and HS codes inconsistent with other containers holding these products. A closer examination showed that these anomalous containers were most likely to have product descriptions of corrugated cardboard, fireworks, glass jars, and clear bottles. More sophisticated algorithms, along with improved information, could help CBP and USCG better prioritize which containers to inspect upon arrival.

Threat Assessment. Machine learning can also be used for threat assessment and conflict forecasting to estimate the risk of a terrorist, cyber, or other threats to the MTS. Threat assessment is a type of supervised learning model. It aims to predict whether information about a given perpetrator signifies a high risk of violence given information about other potentially dangerous actors. Conflict forecasting is another type of supervised learning model; it aims to extrapolate how individual terrorist groups may behave in the future.

A benefit to supervised learning models is that they can often perform feature selection. This provides information about which risk indicators are most important in predicting a given outcome. This information can help analysts sift through large amounts of information to more quickly distinguish the "signal from the noise."

Example: The CIA-funded Political Instability Task Force uses ML algorithms to predict what states are most likely to experience violent revolutions or coup d'etats based on a large variety of potential warning signs.[273] ML algorithms can also be used to predict when a violent incident is likely to occur by looking at previous patterns in the timing of violence.[274] In the maritime domain, stakeholders may be interested in employing computer algorithms to predict whether social media chatter represents a credible threat to use violence.

Target Attribution. Since more actors now operate in the maritime domain, the number of potential malicious actors is constantly growing and evolving. This can make it increasingly hard to trace suspicious activities to specific actors. ML algorithms can learn the "signatures" associated with attacks. This technique can be used to identify which actors are behind probing behaviors—such as phishing or unauthorized UAS usage. It can also be used to more quickly determine the perpetrator behind a terrorist attack after it occurs. When an attack occurs, ML can use information about the signatures—or patterns of behaviors, equipment, and timing—associated with specific attacks to provide a predicted probability about the perpetrator behind the attack. Law enforcement can then use this information in their investigation and response efforts.

Example: Cyber-attacks often vary in their level of sophistication, methods, software, and targets. ML can use this information to discern which attacks are attributable to state actors, hacktivists, script-kiddies, or terrorist actors. Pitropakis et al. (2018) develop a cyber attribution framework to identify parties behind Advanced Persistent Threats (APTs).[275] Their framework applies network analysis and clustering techniques to a variety of open-source information about cyber threats. Spangler and White (2020) use information about claimed terrorist attacks in the Global Terrorism Database to identify which perpetrators are most responsible for the vast number of unknown and unclaimed attacks.[276]

Resilience-Building. A final ML application addresses the potential for "reverse machine learning" in port operations. If port operations and law enforcement efforts are routine and predictable, then NSAs may be able to exploit blind spots in these routines for smuggling and trafficking. First, practitioners can assess the severity

[273] Jack A. Goldstone, Robert H. Bates, David L. Epstein, Ted Robert Gurr, Michael B. Lustik, Monty G. Marshall, Jay Ulfelder, and Mark Woodward. "A global model for forecasting political instability." *American Journal of Political Science* 54, no. 1 (2010): 190-208.
[274] Malone, Iris. "Recurrent Neural Nets for Conflict Forecasting." Working Manuscript.
[275] Nikolaos Pitropakis, Emmanouil Panaousis, Alkiviadis Giannakoulias, George Kalpakis, Rodrigo Diaz Rodriguez, and Panayiotis Sarigiannidis. "An enhanced cyber attack attribution framework." In International Conference on Trust and Privacy in Digital Business, pp. 213-228. Springer, Cham, 2018.
[276] Ethan Spangler and Dustin White. "Terrorist Attack Attribution with Machine Learning based Multiple Imputation." 2020. Available at SSRN 3648711.

of this problem by collecting information on patrols, cargo inspections, and other metrics. They may build a supervised ML model to see whether certain times of the day, locations, employees, or other characteristics predict when and where these incidents occur. Second, practitioners can implement a degree of randomness (e.g. die roll) into when or where these metrics occur. This simple measure should disrupt the routine nature and make it harder for "reverse machine learning" to succeed.

Personnel Training and Operational Exercises

The shifting threat environment of maritime security requires port and ship facilities to prepare for situations of increasing complexity. Interviewees stressed that because anticipating all potential threats in this environment is challenging and time-consuming, emphasis should be placed on developing a robust response capacity. A cornerstone of managing responses is ensuring that the workforce is aware of different threats and the procedures necessary to mitigate, control, and recover from attacks. At the same time, natural human limitations for maintaining heightened attention and awareness could lead to complacency and unintended consequences. Therefore, training and facilitating operational exercises is crucial for establishing expectations for the kind of risk environment employees will operate in, and the security measures they should be prepared to practice and activate when necessary.

Applications for personnel training and operational exercises include:

1. **Deter:** Vulnerability Mitigation
2. **Detect:** Anomaly Detection
3. **Deliver:** Capacity Building, Incident Response

*Vulnerability mitigation***.** Training and scenario exercises are one tool to identify and assess gaps and vulnerabilities in maritime security. Exercises provide insight into the capabilities of employees, security procedures, and physical and digital infrastructure. Participants and stakeholders have an opportunity to then evaluate the strengths and weaknesses of security capabilities, resources, and procedures and address identified vulnerabilities as needed. Conducting operational exercises deters attacks by ensuring that the necessary security measures are in place to reduce the points of vulnerability that adversaries could exploit.

Example: The Cybersecurity and Infrastructure Security Agency (CISA) conducts cyber and physical security exercises with both government and industry partners in the critical infrastructure sector. CISA assists in the design, planning, and execution of these exercises. Their operations-based activities include drills, functional exercises, and full-scale scenarios. Infrastructure security scenarios include active shooter incidents, terrorist attacks, vehicle ramming, and IED attacks. Cyber scenarios include phishing, ransomware, loss of personally identifiable information, and industrial control systems compromise. These exercises are meant to identify best practices, lessons learned, and areas for improvement in plans and procedures. The USCG could integrate expertise from CISA to further develop the scenarios within its Area Maritime Security Training and Exercise Program.

Anomaly Detection. One interviewee stated that "situational awareness is key to understand and detect anomalies." Situational awareness is cultivated through local knowledge and expertise, since those who work on the frontlines of maritime facilities recognize patterns and can contextualize potential threats. Routine training and scenario exercises further support anomaly detection by deepening employees' awareness of specific patterns and anomalies. An interviewee described an example where a customs inspector in the Port of Miami would recognize a shipment of cement from South America as suspicious since cement in Florida is cheap, and there would be no market for it to be imported. Cement and similar industrial cargo could conceal firearms, missiles, hazardous chemicals, drugs, and illicit money. In addition to detecting weapons and illicit goods, facility employees are also on the frontlines of detecting potential cyber-attacks. For example, cybersecurity training could enable individuals to identify phishing attempts via email, one of the most common cyber-attack vectors. This type of situational awareness is gained through experience and bolstered by training and practical

scenario exercises where employees learn how to identify suspicious behavior, cargo, and digital activity. The DHS Soft Targets and Crowded Places Security Plan Overview reiterates that "individuals working in or using a soft target or crowded place, often are in the best position to help detect and prevent possible attacks."[277]

Capacity Building and Incident Response. Practical training and scenario exercises can also enhance the response capacity of stakeholders. For example, trainings with follow-on activities or periodic operational drills can improve the coordination, timeliness, and effectiveness of responses. The USCG works with federal, state, and local partners, each of whom may have different approaches and procedures to the same TSI. Conducting comprehensive trainings and scenario exercises helps ensure that these stakeholders have a cohesive, coordinated response pre-determined before a real-life incident occurs.

Example: Over the last few years, the USCG and its local agencies have conducted active shooter and insider threat exercises across the country. Many of these exercises, including in Puget Sound, Washington,[278] Elizabeth City, North Carolina,[279] and Marietta, Ohio,[280] simulated active shooter incidents on ferry boats. These exercises involved participants from Coast Guard units, the Department of Transportation, the police department, and other relevant partners. During the training, participants practiced tactical procedures, de-escalation methods, and emergency medical responses. USCG should also consider other conducting exercises for various attack scenarios, such as a MIED attack, at multiple locations, such as a handling terminal or waterfront area. For example, the Gulf of Mexico Area Maritime Security Committee conducted an insider threat and cybersecurity attack scenario to test the Area Maritime Security Plan and the security plans of port partners.[281] However, this was only a virtual tabletop exercise due to COVID-19 restrictions.

Wargaming and Simulation Exercises

Beyond their use as a purely theoretical or academic exercise, detailed wargaming and simulation exercises are valuable tools for anticipating the impact of maritime security threats. As discussed in this report, emerging technologies create new entry points and methods of attack, although there is still much uncertainty about how attacks will manifest. Simulations are useful for exploring a range of possible attack scenarios, creating innovative responses and workarounds, and ultimately integrating this information into operations, force design, and doctrine. However, to be effective, the insights gained from wargaming and simulation exercises must be communicated horizontally to relevant maritime security partners and vertically to senior-level managers and decision-makers.

The potential applications of wargaming and simulation exercises include:

1. **Deter:** Vulnerability Mitigation
2. **Detect:** Risk Assessment
3. **Deliver:** Incident Response, Future Research

[277] "U.S. Department of Homeland Security Soft Targets and Crowded Places Security Plan Overview." Department of Homeland Security. May 2018. p.2. https://www.cisa.gov/sites/default/files/publications/DHS-Soft-Target-Crowded-Place-Security-Plan-Overview-052018-508_0.pdf

[278] Thomas Bliss. "Vessel Safety, Security & Response to Hostile Actors." The Northwest Maritime Academy. May 24, 2017. https://northwestmaritimeacademy.com/vessel-safety-security-response-hostile-actors/

[279] Annette Weston. "Coast Guard conducts active shooter training on ferry in North Carolina." ABC News Channel 12. March 5, 2020. https://wcti12.com/news/local/coast-guard-conducts-active-shooter-training-on-ferry-in-north-carolinaMarch

[280] Kirk Moore. "Active shooter exercise on Ohio sternwheeler." Workboat. May 21, 2019. https://www.workboat.com/passenger-vessels/active-shooter-exercise-on-ohio-sternwheeler

[281] CWO Kurt Fredrickson. "Gulf of Mexico AMSC conducts insider threat and cybersecurity exercise." Coast Guard Maritime Commons. November 25, 2020. https://mariners.coastguard.blog/2020/11/25/gulf-of-mexico-amsc-conducts-insider-threat-and-cybersecurity-exercise/

Vulnerability Mitigation. Wargames and simulations are "representations of conflict or competition in a synthetic environment, in which people make decisions and respond to the consequences of those decisions."[282] Additionally, this process "relies heavily on joint doctrinal foundation, tactical judgement, and operational and regional/area experience."[283] In sum, the outcomes of each action, reaction, and counteraction within this synthetic environment depend greatly on "the human factor." A thorough examination of each course of action developed in the wargaming and simulation exercises allows participants to recognize where their assumptions were challenged, unforeseen critical tracks or problems emerged, and how operational design shaped the overall outcome of the scenario, including remaining risks. These details are essential to understanding the strengths and vulnerabilities of stakeholder responses to maritime incidents, which inform future risk reduction and resilience-building measures.

Example: The Jack Voltaic (JV) Cyber Research Project is a bottom-up approach to critical infrastructure resilience through understanding existing cybersecurity capabilities and identifying gaps. In its third and most recent iteration, JV 3.0, JV partnered with the Army Cyber Institute, the Army, and the Department of Defense. JV 3.0 was a city-level exercise that analyzed "how multiple small-scale, cascading cyber-attacks against local municipalities and their commercial critical infrastructure in the strategic port cities of Charleston, SC, and Savannah, GA, could disrupt force projection operations."[284] This simulation took place over two single-day virtual events. As the simulation progressed "by spreading to new areas, organizations, or systems or by causing increasing damage," attribution and incident causes were withheld to facilitate debate among participants about how to respond.

This simulation revealed numerous insights into multi-level and multi-partner cyber vulnerabilities. Some notable findings include: the Army is reliant on various interdependent critical infrastructures which it does not own or operate, making it vulnerable to incidents affecting external actors; interactions and interdependencies between IT and communications technology have created gray-zone attack vectors which have a high impact on MTS operations; there is no standard for cyber incident declaration; the whole-of-community approach to responding to cyber-attacks is not yet effective and coordinated; translating national-level laws and policies to the local level and across states remains a challenge.[285] This simulation exercise yielded practical and actionable policy recommendations to relevant stakeholders, including for the DHS and DOD to expand the USCG Cyber Command's authorizations, resources, and mission to include cyber incident response support for strategic ports. The USCG, and its Cyber Command, should consider participating in these types of simulation exercises to identify and remedy vulnerabilities across its local, industry, and government partners who operate at strategic port locations.

Risk Assessment. Rigorous and detailed wargames are useful risk assessment tools, as they evaluate both the vulnerability and threat elements of the risk equation. Some have criticized that current analysis methods, such as cost-benefit analysis, capabilities-based assessments, and alternative analysis, are predisposed to focus on the vulnerability aspect without accounting for threats posed by the adversary.[286] However, wargaming includes anticipating adversaries' objectives, capabilities, and decisions within the flow of operations, as it informs which course of actions should be selected. Similarly, simulation exercises can integrate complex, multi-layered

---

[282] Joint Chiefs of Staff. "Joint Publication 5-0." December 1, 2020. p. 123. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0.pdf?ver=ztDG06paGvpQRrLxThNZUw%3d%3d

[283] Ibid, p. 126.

[284] "JACK VOLTAIC 3.0. Cyber Research Report Executive Summary." Army Cyber Institute at West Point and FTI Consulting. February 19, 2021. p. 3. https://cyber.army.mil/Portals/3/Documents/JackVoltaic/3.0/JackVoltaic_Executive_Summary_3.0.pdf?ver=nWJUt-NyVHwCdqkbbi7tTw%3d%3d

[285] Ibid, p. 7.

[286] Jeff Appleget, Jeff Kline, and Rob Burks. "Revamping Wargaming Education for the U.S. Department of Defense." Center for International Maritime Security. November 17, 2020. https://cimsec.org/revamping-wargaming-education-for-the-u-s-department-of-defense/

attacks and interactions between adversaries and response personnel. By producing models of various scenarios and courses of action, participants can accurately assess risk, identify priorities, and create contingency plans.

Example: In recent years, there have been numerous occasions of spoofing vessels. However, in 2013, researchers at the University of Texas at Austin successfully spoofed an $80 million private yacht using the world's first openly acknowledged GPS spoofing device.[287] The purpose of the experiment was to determine how difficult it would be for an adversary to carry out a spoofing attack at sea and how easily sensors in the ship's command room could identify the threat. In the simulated attack, the GPS signals from the spoofing device were indistinguishable from the legitimate signals. The team, acting as the adversary, was subtly able to coerce the ship onto a new course without the navigation system accurately determining the location discrepancy. Years before an actual attack, this simulation demonstrated the gap between the capabilities of GPS spoofing devices that adversaries may employ and those aboard the vessel that mariners use. This threat persists as technology advances, and navigation systems remain vulnerable. Today, GPS spoofing devices are interfering with more consequential vessels, including military ships.

Incident Response and Future Research. Another advantage of simulations and wargames is that they provide participants with a deeper understanding of a problem and the potential solutions. These exercises help manage uncertainty by reducing complex issues to several critical factors. The outcomes help determine viable options for how to respond to challenges and signal areas of future research, investment, and collaboration. When such activities are iterated and coupled with other learning exercises, such as fielding exercises, participants are able to verify their findings.

Example: The robust UAS program that ISIS had developed was short-lived and relatively ineffectual against American forces. This was because years prior, in 2008, the U.S. Army's Asymmetric Warfare Group had "identified UASs as a viable threat and deployed counter-UAS training, technology, and tactics to Army units in combat."[288] In 2014, the Asymmetric Warfare Group assessed that ISIS' program was expanding rapidly, leading to field-driven adaptation. The group began conducting experimental exercises with armed commercial UASs to test their capabilities and limitations, particularly how effective a UAS would be as a munitions delivery system. The results of these simulations were shared with American forces in Iraq and "integrated" into Army training centers to educate all U.S. Army forces on counter-UAS capabilities. In addition to helping develop technical countermeasures, the simulation and combat experiments yielded insight into the tactical adaptations that could disrupt UAS capabilities entirely, at no extra cost. Interviewees stressed that non-state actors' ability to adapt remains a persistent challenge to maritime security. The Asymmetric Warfare Group's success illustrates the value of simulating, testing, sharing knowledge, and scaling solutions to deliver effective responses against asymmetric threats.

Regulations

Interviewees and research stressed that there are significant gaps in port security regulations, specifically in addressing the emerging threats and vulnerabilities outlined in this report. For example, while cyber threats are beginning to be recognized at the institutional level, there is still much uncertainty regarding the prevalence of cyber-related standards. This issue will become more acute as other digital technologies are integrated into vessel and port operations. As far as emerging technologies, their use has far outpaced regulations. For example, while the FAA prohibits drones from entering within a 5-mile radius of an airport, no such provision exists for other critical infrastructure like ports. Updating regulations and adopting new ones are necessary for establishing a shared approach to the threats that all port security stakeholders face. While implementation is a secondary challenge, regulations ground the pertinence and effectiveness of adopting measures to mitigate risk.

[287] "UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea." UT News. July 29, 2013. https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/
[288] T.S. Allen, Kyle Brown, and Jonathan Askonas. "How the Army Out-Innovated the Islamic State's Drones." War on the Rocks. December 21, 2020. https://warontherocks.com/2020/12/how-the-army-out-innovated-the-islamic-states-drones/

The potential applications of maritime security regulations include:
1. **Deter:** Address Compliance Gaps
2. **Deliver:** Capacity Building

Address Compliance Gaps. Following September 11, the United States adopted new international standards, national laws, and industry regulations to protect maritime infrastructure and trade. However, in recent years, regulations have not kept pace with emerging threats to maritime security, particularly within the cyber domain. There have been notable developments regarding managing cyber risks, including the IMO releasing a new set of guidelines on maritime cyber risk management, the USCG releasing a Navigation and Vessel Inspection Circular (NVIC 01-20) concerning "Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities" in February 2020, and the USCG updating its Cyber Strategic Outlook in August 2021. While these documents are helpful frameworks to mitigate cyber threats, interviewees expressed that vessels and facilities remain vulnerable to cyber threats because these regulations lack an operational focus.

For example, the NVIC 01-20 is not prescriptive, as it "does not include a checklist or otherwise prescribe cyber security solutions."[289] While this approach allows for flexibility, which is important, it also creates gaps in how facilities analyze vulnerabilities in their Facility Security Assessments and address them in their Facility Security Plans. Moreover, the NVIC 01-20 only applies to MTSA-regulated facilities, not vessels. Conversely, the IMO guidelines only apply to vessels, not port facilities. Future iterations of cyber risk management regulations need to meet the scale and scope of the cyber domain. Similar regulations regarding small vessel traffic should also command attention. This means establishing, at least, baseline operational requirements for *both* vessels and ports, and ensuring consistency between national and international regulatory frameworks. Formal guidelines are a critical start, but effectively addressing cyber risks requires implementing standards that are enforceable and uniform.

Capacity Building. Interviewees stated that one of the structural challenges to enforcing uniform regulations for vessels, cargo, and operators are the conflicting regulations between the nations that operate a ship and those that own a ship. Shipowners and flag states may also fail to comply with regulations stipulated by domestic and international instruments, such as the ISPS Code. This makes vessels vulnerable to the trafficking of illicit cargo by transnational criminal organizations and violent NSAs. However, as programs like C-TPAT and CSI demonstrate, effectively protecting U.S. ports from external threats requires multilateral security cooperation with global trading partners. These efforts include developing shared and integrated approaches to regulations, inspections, information sharing, and other security procedures. Improving the USCG's capacity to secure U.S. ports and maritime infrastructure while ensuring the continued flow of commerce requires continued global collaboration.

Example: Port Security Control (PSC) is the examination of "foreign ships in national ports to verify that the condition of the ship and its equipment comply with the requirements of international regulations and that the ship is manned and operated in compliance with these rules."[290] PSC allows ships to be inspected by state authorities at foreign ports, including without consulting flag states. The nine regional agreements on PSC—Memoranda of Understanding (MoUs)—establish an agreed-upon inspections mechanism to ensure that ships at MoU members' ports are inspected, and if they are found to be non-compliant, flag states must address substandard ships. The Paris MoU, which includes European and North Atlantic countries, also established an Information System. All MoU members have access to information on PSC inspections and port call data, ship

[289] "Navigation and Vessel Inspection Circular (NVIC) 01-20; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities" Federal Register. March 20, 2020. https://www.federalregister.gov/documents/2020/03/20/2020-05823/navigation-and-vessel-inspection-circular-nvic-01-20-guidelines-for-addressing-cyber-risks-at
[290] "Port State Control." International Maritime Organizations. https://www.imo.org/en/OurWork/MSAS/Pages/PortStateControl.aspx

risk profiles, companies' performance, and other functionalities.[291] A shared information system encourages compliance. PSC leverages the fact that ports are natural chokepoints where port jurisdiction allows authorities to "monitor and control poorly regulated flag-of-convenience ships suspected of involvement in destabilizing commodity flows."[292] PSC standardizes regional training and inspection techniques, so Members can jointly monitor sub-standard ships and crew while also avoiding multiple unnecessary inspections for compliant vessels.[293] After overcoming the initial challenge of understanding Member States' regulatory system, PSC regimes are effective multilateral mechanisms to facilitate information sharing and cohesive maritime governance.

Reflection and Lessons Learned Series

The threat environment has shifted drastically since the creation and implementation of post-9/11 port security measures. While threats of maritime terrorism, drug trafficking, and piracy persist, they are likely to manifest in nonconventional ways. Organizations, companies, and individuals worldwide have—either through necessity or good business practice—found new ways to analyze the threats and vulnerabilities within their operating environment and manage these risks effectively. This section will highlight some key lessons learned interviewees articulated and current examples of protecting critical maritime infrastructure.

Selected lessons learned included in this section apply to:
1. **Deter:** Vulnerability Mitigation
2. **Detect**: Information Sharing
3. **Deliver:** Incident Response

Vulnerability Mitigation. Interviewees commonly cited two challenges to risk management: a lack of expertise and bifurcated security culture. While security personnel may have valuable knowledge about the operational aspects of their ports, there is a lack of human resources and expertise regarding emerging technology, including cybersecurity and automated systems. A related challenge is that there are many stakeholders in the maritime industry, each of whom has different risk mitigation capabilities and systems. As some port authorities have demonstrated, a potential strategy to overcome these technical complexities is establishing a centralized entity that provides in-house expertise while also convening stakeholders to develop a common approach to risks associated with cyber and other emerging technologies. These entities operate under the premise that ports are an ecosystem of private companies, government entities, crew and facility personnel, and digital and physical infrastructure. In-house efforts to mitigate vulnerabilities must be complemented by efforts to address the vulnerabilities at points of overlap between stakeholders. Managing cyber threats, for example, means that this centralized entity must create a culture that optimizes the ecosystem's interdependence on digitalization and automation while concurrently enhancing the digital resilience within and between these partners.

Example: The Rotterdam Port Authority launched FERM in 2016 as a part of Rotterdam's Port Cyber Resilience Program. FERM raises awareness about digital vulnerabilities and risks among organizations of all sizes in the Port of Rotterdam.[294] FERM participants have access to an IT portal for interaction and knowledge sharing between participants, information about current threats and response measures, cyber risk scans, newsletters, joint training exercises, and annual crisis exercises.[295] FERM also periodically hosts "Port Cyber Cafes," an informal event where experts from the field discuss a current topic around cybersecurity in the

[291] "Paris Memorandum of Understanding on Port State Control." Paris MoU. p .14. https://www.parismou.org/sites/default/files/Paris%20MoU%20including%2043rd%20amendment%20final.pdf
[292] Aaron Davenport. "Lessons from Maritime Narcotics Interdiction." RAND Corporation. November 5, 2020. p. 17. https://www.rand.org/pubs/external_publications/EP68327.html
[293] "Port State Control." International Maritime Organizations. https://www.imo.org/en/OurWork/MSAS/Pages/PortStateControl.aspx
[294] "What is FERM." FERM Rotterdam Port Cyber Resilience. https://www.ferm-rotterdam.nl/index.php/nl/wat-ferm
[295] "Samen sterk in cyberweer-baarheid." FERM. https://www.ferm-rotterdam.nl/sites/default/files/2021-08/FERM%20infographic.pdf

Rotterdam Port Area.[296] Topics at the Cafes have included "Drones and Security," "Human Factors," and "Espionage and IT Vulnerabilities." In addition to providing expert resources for organizations to improve their cyber resilience, FERM is a platform for port stakeholders to share, learn, and exercise cybersecurity. Through digital and social networks, FERM is creating a culture of cyber resilience within its port ecosystem, which USCG should consider emulating in strategic U.S. ports.

Information Sharing. Another lesson that interviewees emphasized was the importance of a platform for information sharing, particularly one that informs both government and industry stakeholders. Given the inherent link between maritime security and global commerce, private companies also need access to updated, reliable information on current concerns and threats. While certain threats may have a more far-reaching impact, such as the Colonial Pipeline shutdown, which requires national-level information sharing, interviewees expressed that a platform at the local or regional level provides more specific and actionable information. However, a precondition for sharing helpful information to all partners in a port ecosystem is establishing trust with stakeholders, especially private companies that may be reluctant to share information. In addition to initiating personal connections, creating a network of trust requires framing information sharing as mutually beneficial. For government stakeholders, reliable intelligence strengthens maritime security, and for private entities, maritime security preserves the continuity of their business.

Example: At the Port of Los Angeles and Long Beach, there are two examples of effective information-sharing platforms for government and industry partners. First, the Marine Exchange Southern California is a non-profit organization that partners with the USCG and state and local government agencies to provide vessel traffic and maritime information to four regional ports.[297] The Marine Exchange compiles and disseminates vessel activity information to the local maritime industry and waterfront business community.[298] Additionally, as the only public-private partnership for Vessel Traffic Service, the Marine Exchange collaborates with USCG to manage the movement of vessels, facilitate rule enforcement, and detect anomalies. By efficiently and reliably providing information to the USCG, government agencies, and port stakeholders, the Marine Exchange strengthens maritime domain awareness within and between four ports in Southern California. A second example is the Marine Safety Information Bulletins, with specific supplements on cyber-related risks. The newsletter includes cyber threats to be aware of, cyber hygiene practices, and recent cyber incidents without disclosing company-specific information. The newsletter contains details about cyber threats within the LA/LB community and information about cyber risks within the critical infrastructure sector in general. Since many cyber risks emerge from human behaviors, newsletters are a simple but effective way to raise collective awareness on cyber-related risks.

Incident Response and Resource Acquisition Times. As the threat and ubiquity of the cyber domain and emerging technologies continue to grow, regaining a competitive advantage by developing and acquiring new capabilities has become imperative to maritime law enforcement. In a 2018 report, the Government Accountability Office found that the Coast Guard makes trade-off decisions regarding acquisitions during its annual budget process, and that this leads to a "build-up of near-term unfunded acquisitions."[299] These findings were foreshadowed by the 2010 devolution of the Deepwater project due to underdeveloped acquisition management capabilities. The hard-learned lesson is that the Coast Guard has been, and will continue to be, in need of improvements to its resource acquisition process to access the technologies necessary to respond to emerging threats. Resource acquisition must be timely, flexible, and risk-informed.

---

[296] "FERM Port Cyber Cafes." FERM. https://www.ferm-rotterdam.nl/port-cyber

[297] "Mission Statement." Marine Exchange Southern California. Last Updated April 11, 2018. p. 9. https://mxsocal.org/assets/pdf/mx-socal-mission-statement-with-change-1-dated-11-apr-20182.pdf

[298] Ibid, p. 9.

[299] "Coast Guard Acquisitions: Actions Needed to Address Longstanding Portfolio Management Challenges." U.S. Government Accountability Office. July 24, 2018. https://www.gao.gov/products/gao-18-454

Example: U.S. Army Special Operations Command (SOCOM) uses a middle-tier acquisition model called "buy-try-decide."[300] Middle-tier acquisition is a mechanism that allows the military to "soft start" a new program or accelerate the prototyping of an existing program so personnel can test prototypes and provide feedback as product development continues.[301] This model allows SOCOM personnel to evaluate the functionality of a product, predict formal acquisition and sustainment costs, identify potential alternatives, and pilot product integration into the organization. In the short term, this means that SOCOM can acquire at least some version of a new capability it needs, and in the long term, it means industry partners get valuable feedback on whether to modify or cancel a product to meet end-users' needs.

SOCOM has the benefit of being a smaller military organization, so "the lack of bureaucratic overhead allows it to identify emerging issues, modify programs that are underway, or, in certain cases, divest from programs more rapidly."[302] Additionally, because its programs have a lower dollar threshold than other services and therefore receive less statutory and regulatory scrutiny, SOCOM has a "culture of innovation and risk-taking" in its acquisition programs.[303] Finally, SOCOM also has "a more focused, operations-oriented acquisition culture." The USCG could leverage the same benefits of being a smaller, maritime-focused organization by implementing the "buy-try-decide" model. This process usually takes place within a single financial year, which compresses the resource acquisition timeline without compromising on the technical experimentation necessary to reach the optimal final product.

Conclusion

How has port security evolved since 2001, and what challenges exist moving forward? This report provides an overview of the current state of port security, new risks that have arisen since 9/11 and the 2002 Maritime Transportation Security Act, the types of security challenges these risks pose, and how practitioners may mitigate these challenges.

Based on a series of interviews and in-depth research, we find that increasing vessel traffic, the growing role of small actors below the nation-state threshold, and the rising number of MTS stakeholders has led to an increasingly complicated threat environment. Emerging threats challenge existing domestic capabilities due to an increasingly diffuse and unorganized set of extremist actors' intent on using violence, increasingly sophisticated cyber-attacks and other advanced persistent threats, and non-state adoption of advanced technologies and weapons systems. The report also identifies a growing number of vulnerabilities among ships, ports, and people whereby these threats can manifest.

The combination of an increasingly diverse threat environment with an increase in vulnerabilities results in a different set of security challenges for the maritime domain. We identify that today's security environment poses five major challenges, including new domains for exploitation, attribution challenges, big data and information processing, new information and communication technologies, and globalization and increased interdependence. We argue that, unlike the threat environment immediately following 9/11, emerging risks to the MTS are driven by higher probability, but lower magnitude incidents. Our recommendations to harness these challenges and improve resilience include investments in a range of strategies which collectively can help secure the MTS.

---

[300] COL Robert Bailey. "Rapid, Smart, and Flexible Acquisition." Marine Corps Gazette. 2020. https://mca-marines.org/wp-content/uploads/Rapid-Smart-and-Flexible-Acquisition.pdf
[301] Joel D. Babbitt and Donald Schlomer. "The Need for Speed." U.S. Army. April 25, 2019. https://www.army.mil/article/220883/the_need_for_speed
[302] Moshe Schwartz and Jason A. Purdy. "United States Special Operations Command Acquisition Authorities." Congressional Research Service. p. 9. July 9, 2018. https://fas.org/sgp/crs/natsec/R45252.pdf
[303] Ibid, p. 9.