A Framework for Cybersecurity Assessments of Critical Port Infrastructure

Daniel Trimble, Jonathon Monken, & Alexander F. L. Sand
Madison Policy Forum

31 August 2016

All statements of fact, opinion, or analysis expressed are those of the authors and do not reflect the official policy positions of the U.S. Department of Defense, U.S. Coast Guard, any other agencies of the U.S. government, or PJM Interconnection.

ABSTRACT

Nearly all global economic trade flows through the ports and maritime infrastructure. A majority of that infrastructure in many countries is privately owned and operated. Consistent with international treaties and legislation, government and industry stakeholders are responsible for the physical safety and security of this maritime domain. The majority of this government oversight and industry cooperation focuses on physical access and the safe construction and operation of ships. The cybersecurity of critical maritime infrastructure, however, remains largely unregulated with minimal, if any, assessment or mitigation of cybersecurity risks. Operators of maritime infrastructure face significant challenges with legal and statutory limitations balanced against existing standards in other critical infrastructure sectors.

Maritime infrastructure encompasses industrial control, SCADA, and information technology systems—much of it proprietary with few common technology or implementation standards. Most are dependent on infrastructure in intersecting domains, from energy to transportation. Despite this dependency, operational coordination and joint cyber risk assessment with "upstream" infrastructure is rare. While many operators of the infrastructure are concerned about cybersecurity, the complexity of their systems, interdependence with other sectors, and significant global interests in mitigating cyber risks against such crucial economic arteries demonstrates a compelling need for standardized frameworks for assessing cybersecurity risk in the maritime domain.

Our work identifies cyber risk factors affecting maritime infrastructure, present barriers to mitigating risks, and regulatory models for implementing a standardized framework for addressing these risks. Finally, it proposes a model for an independent, non-governmental entity to conduct cybersecurity assessments of critical maritime infrastructure.

ABOUT THE AUTHORS

Dan Trimble fuses experience in tech product development, marketing, policy, and international affairs to help cultivate new technologies, policies, and public/private partnerships for solving pressing public challenges. Earlier, he ran cyber analysis teams in the U.S. intelligence community; has served as a U.S. Coast Guard Reserve intelligence and disaster response officer for more than 12 years; and has spent the better part of 20 years helping tech companies bring their products to market. He also served as executive director of an advocacy organization facilitating public/private partnerships to strengthen entrepreneurship and innovation. A student of international business, government, and international relations, Mr. Trimble has studied at the National Intelligence University, U.S. Naval War College, the Joint Forces Staff College, and Golden Gate University. Based in California, in his spare time he's a published photographer and avid traveler.

Alexander F. L. Sand is an experienced public and private sector cybersecurity and virtual currency attorney, in addition to experience investigating improper practices within the spot foreign exchange market. Earlier in his career, he was an Associate at Shipkevich, PLLC where he advised clients seeking to register with the CFTC regarding regulatory requirements arising under the Dodd-Frank Act. He also worked on investigations related to residential mortgage-backed securities, indenture trustees, and insurance pricing. Alexander received a B.A. in History from Stony Brook University, and a J.D., cum laude, from Hofstra University School of Law, where he was an editor of the Hofstra Law Review.

Jonathon Monken is the Senior Director, System Resiliency and Strategic Coordination for PJM Interconnection. He works in the areas of business continuity, physical and cyber security, risk management, and resilience planning for the world's largest wholesale energy market. Mr. Monken also served four years as Director of the Illinois Emergency Management Agency (IEMA) and two years as Acting Director of the Illinois State Police and possesses a distinguished military career having served as an armor officer for one tour of duty in Kosovo and two combat tours in Iraq. Monken earned a Bachelor of Science from the United States Military Academy at West Point, and holds a Masters in Business Administration from Northwestern University's Kellogg School of Management.

Table of Contents

Executive Summary

Nearly all global economic trade flows through the ports and maritime infrastructure. This infrastructure encompasses industrial control, SCADA, and information technology systems—much of it proprietary with few common technology or implementation standards. Maritime infrastructure also has a particularly critical dependence on infrastructure from the energy and transportation sectors. Despite this deep interdependency, operational coordination and joint cyber risk assessment with up- and down-stream infrastructure is rare. While many operators of the infrastructure are concerned about cybersecurity, the structure of ports and port operations, complexity of their systems, deeply-entangled interdependence with other sectors, and other emerging threats create significant challenges in mitigating cybersecurity risks.

Consistent with legislation and international treaties, there is strong, codified government oversight and regulation addressing maritime port security in the United States and overseas. However, these regulations are targeted at ensuring the physical safety and security of the maritime domain. The same is true of the standards set by private international safety rating groups known as classification societies. The cybersecurity of critical maritime infrastructure remains largely unregulated with minimal, if any, assessment or mitigation of cybersecurity risks.

The significant cybersecurity risks facing the maritime domain, the lack of clear standards and requirements addressing cybersecurity of maritime infrastructure, and significant global interests in mitigating cyber risks against such crucial economic arteries demonstrates a compelling need for standardized frameworks for assessing and mitigating these risks.

This paper focuses on cybersecurity policy in the maritime domain, not technical analysis. Extensive work has been done by scholars and security experts throughout the world on the technical vulnerabilities and attack vectors faced by critical infrastructure, including the specific types of components and systems noted in this paper. Of particular note, the work of Dr. Bonnie Zhu et. al. at the University of California[1] offers an excellent primer relevant across critical infrastructure sectors. The U.S. National Institute of Standards and Technology (NIST) has also published relevant studies[2], with an extensive library of additional resources available through SCADAhacker.com[3]. Recent DHS-CERT reporting also offers examples of "BlackEnergy" malware targeting specific common commercial

[1] Bonnie Zhu, Anthony Joseph and Shankar Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems, University of California at Berkeley, 19 October 2011, https://people.eecs.berkeley.edu/~adj/publications/paper-files/ZhuJosephSastry_SCADA_Attack_Taxonomy_FinalV.pdf.

[2] Keith Stouffer, Joe Falco, and Karen Kent, "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security", National Institute of Standards and Technology, NIST Special Publication 800-82, September 2006, https://www.dhs.gov/sites/default/files/publications/csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf.

[3] Joel Langill, "Library of Resources for Industrial Control System Security", SCADAhacker.com, January-March 2016, https://scadahacker.com/library/.

industrial control systems from General Electric, Advantech, and Siemens[4]. The paper assumes some level of familiarity with the technical workings and potential vulnerabilities found within common critical infrastructure components as it examines how best to mitigate those risks from a policy standpoint.

This paper was not intended to identify or evaluate cyber vulnerabilities within critical infrastructure software, hardware, or networks, nor the state or non-state cyber actors likely capable of exploiting them. Its intent is to evaluate authorities and policies for the assessment of cyber risks in the maritime domain, and whether current national policy allows for its effective risk mitigation.

We begin with an examination of cybersecurity risks in the maritime environment. Though it looks at the maritime domain holistically, the paper particularly emphasizes shore-side critical infrastructure of ports and port operators over the cybersecurity factors at play with ships and military facilities. It evaluates the regulatory structures and mechanisms in place today for addressing them, and recommends the creation of a new public/private Maritime Cyber Assessment Organization ("MCAO"). MCAOs would, jointly with public and private sector stakeholders, establish cybersecurity standards specific to port infrastructure and its interconnected systems throughout the intermodal transportation system. MCAOs would implement programs for assessing and enforcing compliance with those standards. Given the reality of constrained resources, political challenges, and the importance of finding collaborative solutions for private sector vulnerabilities with significant public stakes, the MCAO model is proposed to operate within the constraints of existing legislation and regulatory authorities.

[4] Industrial Control Systems Cyber Emergency Response Team, Alert (ICS-ALERT-14-281-01E), United States Department of Homeland Security, updated 02 March 2016 based on original 10 December 2014 report, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

Cybersecurity Risk in Maritime Critical Infrastructure

For all the unprecedented growth in transportation technology, distribution, and industry over the past century, maritime shipping remains the source of 90% of all global commerce, and is central to the economic activity of nearly every nation.[5] By tonnage, within the United States alone, 70% of all imported goods and 76% of all exports are shipped via water. Despite the enormity of this volume, the vast majority occurs at only 300 commercial ports.[6]

The infrastructure required to support this kind of scale across maritime and intermodal transportation sectors is deeply intertwined with globally-connected, public and private networks. Its global reach means 60% of U.S. ports are at least partially owned or operated by foreign corporations or countries, and as many as 80% among America's largest ports.[7] In point of fact, few American companies operate cranes or move containers within the ports; foreign companies are ushering American goods from ship to shore and vice versa. These foreign entanglements have long raised the ire of politicians around security. How should a country weigh the economic benefits of transparent, accessible global commerce with the need to protect against the national security risks of globally-connected, economically-critical network infrastructure? The problem is complicated by direct foreign investments in which foreign corporations and countries invest directly in U.S. interests; foreign entities who may not necessarily have the best interests of America's national security in mind.[8] Because of the scale, complexity, and interconnectedness of this global maritime infrastructure, U.S. ports face significant physical and cybersecurity risks that threaten to significantly disrupt the smooth function of U.S. global and domestic commerce.

Although maritime is not the only economically-critical sector in the U.S. with vulnerable, globally complex infrastructure requirements, it is uniquely situated for cyber risk. As a comparison, the Federal Aviation Administration's National Plan of Integrated Airport Systems notes there are 3,300 commercial airports in the United States, of 20,000 airports in total.[9] However, the highly concentrated nature of maritime ports of entry is potentially a far graver vulnerability. There are only 300 commercial and 600 small ports in the U.S. This is 3.5 times fewer than airports; a level of geographic concentration and potential network isolation that may afford easier access due to the reduced attack surface— especially when considered in the context of foreign influence of the commercial ports already handling the bulk of all economic activity.

---

[5] International Maritime Organization, Overview & Partnerships, accessed 16 August 2016, https://business.un.org/en/entities/13.

[6] Oak Ridge National Laboratory, Freight Analysis Framework Version 3, Data Tabulation Tool, accessed July 2012, http://faf.ornl.gov/fafweb/ Extraction4.aspx.

[7] Laura Meckler and Daniel Machalaba, "Port Deal: Not a Foreign Idea", Wall Street Journal, 09 Mar 2006, http://www.wsj.com/articles/SB114187419573393377.

[8] Eben Kaplan and Lee Hudson Teslik, "Foreign Owners of U.S. Infrastructure", Council on Foreign Relations, 13 Feb 2007, http://www.cfr.org/business-and-foreign-policy/foreign-ownership-us-infrastructure/p10092.

[9] U.S. Waterborne Commerce Statistics Center, "2010 Summary of Domestic and Foreign Waterborne Commerce," May 2012.

Taken a step further, risks identified within a port in the U.S. are more than just risks to that port and its *domestic* extended supply chain and intermodal transportation networks. Wins, losses, and compromises against those domestic risks are *felt globally*: ports and extended supply chains anywhere in the world that do business with, in, or through that U.S. port stand to gain or lose a great deal. It is a globally-shared risk, whether physical or cyber.

In the years after the September 11th attacks, legislative and regulatory efforts were implemented to secure physical access to ports, port infrastructure, and the companies operating in those ports, both in the United States and overseas. Today, ports are more secure than ever before, but emerging threats have given rise to significant cybersecurity risks that have yet to be identified and mitigated in the same way physical risks have been. This expanded attack surface and increased risk profile means that a successful cyber-attack against maritime infrastructure is an increasingly likely occurrence. At some point, such an attack may have sweeping, unmitigated consequences to the U.S. as well as the huge range of actors around the world with a stake in the efficiency, efficacy, or continuity of its maritime operations. A significant cyber-attack against such infrastructure here in the U.S. would be a cyber-attack felt everywhere.

To achieve the significant gains in physical security of the maritime domain since September 11th, sweeping costs have been borne by industry and the public sector. Billions of investment dollars have been spent by ports and operators on security and communications systems, training, personnel, access control systems, threat detection and response platforms, and other priorities. Billions more have been spent by government agencies to oversee maritime security in the ports; train and equip special response forces, law enforcement, and intelligence personnel; and fund grant programs to help ease some of the costs and invest in first responders. The collective global investments in maritime security have been worthwhile, but this is only half the battle. The complexity of cybersecurity assessments means they may be costly to implement. Industry cannot bear all of these costs, and neither can government. Part of the recommendations established later in this paper is to propose a means of conducting thorough cybersecurity assessments without over-burdening any of the stakeholders in the maritime domain; spreading the costs around more efficiently than any public or private entity could achieve on its own.

If we hope to keep at bay the cyber risks faced by U.S. ports, it is imperative that we identify how those risks are identified and assessed, the factors and challenges that give rise to them, and the potential costs of failing to address them.

Structure of Ports and Port Operators

One significant factor giving rise to cybersecurity risks to U.S. ports is the structure of ports and port operations itself. Accordingly, understanding the scale and complexity of the maritime domain's infrastructure and its interconnectedness across sectors first necessitates an understanding of how ports are organized.

The entities that are generally called "ports" or "port authorities" are not necessarily the same entities that conduct activity in the ports. Put another way, some ports are *owned* by one entity while *operated*

by one or more entirely different entities. There are some ports operated and managed by the owner of the port itself, such as in Savannah, Georgia.[10] However, in general, the larger the port, the more likely the port owner operates little to nothing within the port itself. These are often called "land-leasing ports", typically overseen by a local, regional, or state agency or a board of elected or government-appointed officials. Their core business is to lease government-owned land and/or facilities to operating companies who compete for contracts to run port operations. These companies, in turn, track and move ships, cargo, or other goods in and out of the port and keep it all running day-to-day. For purposes of this paper, we will refer to these companies and their subcontractors as "port operators". We will use "ports" to refer to the entities that do not operate actual port capabilities; they lease land/facilities to those companies, and/or manage the total port construct itself.

The varied structure of ports and the diversity of port operators responsible for their activity without common security or reporting standards creates substantial cybersecurity risk. Our research and direct interviews have found that many of these ports—even among the largest and most well-financed—have limited insights, if any, into the critical infrastructure their tenant port operators install or use. Tenants are often free to build out whatever infrastructure is required to support their objectives, with no process for approvals let alone security oversight by interested port or public stakeholders. As is nearly always the case with critical infrastructure, it is privately paid for, owned, and operated; outside intervention is often deemed inappropriate. That problem is compounded by the understandable tendency for private companies to want to avoid public airings of their internal vulnerabilities. However, we live in a 21st century world where a vulnerability to their networks is a risk potentially shared by others.

These structural issues also create additional risk arising from foreign-owned entities that act as port operators in U.S. ports. While the fact that a port operator is foreign-owned does not necessarily mean it is an automatic risk or even viewed by the host country as inherently suspicious, it does allow for potentially easier insider accessibility to cyber-attack vectors. Foreign governments are more likely to have financial or other ties to foreign-owned entities that make them more susceptible to the demands and pressures of a foreign government, who may have a political or national interest in disrupting port operations. Foreign port operators are additionally more likely to utilize systems and networks that fall within the domain of foreign nations without the benefit of U.S. legal protections that protect against the surveillance and appropriation of sensitive data. The international ties and interconnectedness of port operators, in line with the global scale of maritime commercial infrastructure, means that U.S. ports are more connected and exposed to foreign nations and entities that have a demonstrated track record of engaging in malicious activity against U.S. interests. This creates real risks that U.S. ports have to be able to address.

The technology underpinning this diverse range of ports and operators in the maritime domain can be broadly divided into two categories: that of the port itself (typically internal business systems), and that of port operators (such as industrial control systems for monitoring and managing operations, and connected "Internet of Things" devices like cameras and sensors that feed information via wireless to smartphones, tablets, or computers). Additional categories are also important, such as satellites that

[10] Laura Meckler and Daniel Machalaba, "Port Deal: Not a Foreign Idea", Wall Street Journal (paid subscription required), 09 March 2006, http://www.wsj.com/articles/SB114187419573393377.

offer precision navigation and timing capabilities nearly all infrastructure depends upon. However, this paper generally focuses on the technology within the port and port operator's direct control.

The complexity and scale of internal business systems can encompass a wide range of software, hardware, and network connectivity. These can include simple servers or software for relatively small ports, to complex enterprise platforms running on highly scaled, multi-location data centers with hundreds of servers. They generally enable important (and sometimes critical) business functions from invoicing port operators or customers to handling payroll for employees; from business communications to enterprise resource and financial planning, disaster recovery and reconstitution, even police dispatch and 9-1-1 systems.

Although this paper primarily evaluates cyber risk and assessment models of the industrial control infrastructure more common to port operators, it is worth noting the cybersecurity risks inherent in these port business systems can be just as mission-critical. Operating infrastructure will control more direct port operations such as moving cranes, tracking ships, and transferring containers from one transport mode to another (e.g. from a ship to a train). Business systems, on the other hand, may arguably be limited to effects on payroll, administrative functions, or security, for example. However, a cyber-attack against the port's business systems could still make the underlying port operator facilities too accessible/insecure, or foster an environment in which operators are unable or unwilling to conduct business because the ability to book or move cargo at the port-level has been degraded or denied. Accordingly, an effective port cybersecurity assessment must carefully consider the risk posed to internal systems beyond those visible to public or government stakeholders in the normal course of operations. But it must also carefully consider the direct operating and control systems that ensure goods move from point A to point B.

Put another way, we argue any assessment model—government or private—that attempts to assess or mitigate cyber risk in the maritime domain will be woefully inadequate if it does not evaluate both the operating infrastructure and the port's business systems as co-dependent. And as noted earlier, although port and operator infrastructure are typically privately owned wherein private interests and sensitivities should be rightfully protected, a policy failure of government stakeholders to suitably mitigate risk in either area likely leaves unattended security vulnerabilities open for exploit.

The notion of exploiting port and port operator systems to malicious ends is not theoretical. In late 2013, drug traffickers were discovered to have been conducting cyber operations against the Port of Antwerp for two years. The U.S. Department of Homeland Security and CyberKeel, a maritime cybersecurity consulting firm, reported the smugglers gained entry into remote access terminals used to control container movement within the port, installing keyboard and monitor loggers to achieve persistent access. This access vector was used to find and redirect containers of drug shipments as they arrived in the port, moving them onto trucks the smugglers controlled themselves. In at least three other incidents, armed with assault weapons, smugglers were also able to use this access to find their shipments on other trucks leaving the port, and hijack them for the illicit cargo. Because the cyber tools the smugglers installed in the remote terminals enabled them to remotely modify manifest lists provided by shippers, they were able to delete any record their containers ever existed—even the truck

driver didn't know they were carrying more than a ton of cocaine, guns, and 1.3 million Euro.[11,12] Given the lack of assessment oversight, there is little reason to believe this same scenario could not just as easily occur in most other ports. The threat is also not limited to drugs. Similar tactics and techniques could be used for a range of other cyber-enabled transnational crimes or terrorist activity, such as human trafficking, or nuclear or biological weapons smuggling.

Critical Infrastructure Complexity

Unlike humanity's long-entrenched worldview shaped by geographic, physical borders, cyber, by definition, has none. Data moves across IT lines from San Francisco to Dubai in seconds or less. It doesn't stop at the border of countries to ask permission to enter. Meanwhile, networks in one sector may be directly connected to others to enable critical capabilities or more efficient information flow, irrespective of the jurisdiction the systems within those networks are located. This interconnectedness is at the heart of the challenge of mitigating attack models like the lessons learned in Antwerp.

One of the more common components of a port operator's critical infrastructure is Supervisory Control and Data Acquisition systems, or SCADA. Broadly, SCADA refers to specific parts of a broad category of systems known as Industrial Control Systems (ICS). They are lynchpins in tying the varying capabilities of systems, networks, and industrial functions together. Collectively, ICS components manage the processes, execution, and safety behind particularly complex industrial operations. SCADA systems enable remote and on-site access to real-time data about how equipment, pipelines, systems, or other sensors are performing. They allow users to remotely monitor those sensors and equipment inputs; issue commands to change operational performance; and make more informed decisions that balance the needs of safety, security, and operational efficiency.

The idea of remote sensing and control capabilities dates back to the first half of the 20th century, originally based on the idea of connecting a user at one location to equipment at a remote site through connected wires or multi-pair cables. Over the years, it evolved into switch systems, relay systems, and eventually into digital, computerized SCADA systems. The fundamental premise was always that control of equipment and facilities could be conducted remotely. Prior to the 21st century invention of Ethernet and Internet networking protocols like TCP/IP, and wireless technologies like Bluetooth and 802.x "Wi-Fi", this remote access was still relatively geographically-constrained in that the distance it could handle was significantly shorter. This imposed a built-in isolation that protected systems from outside influence or attack by virtue of being geographically harder to access. However, since 21st century networking technology allows access from anywhere in the world at any time, physical proximity is no longer a

[11] U.S. Department of Homeland Security, Customs and Border Protection, "Best Practice—Port of Antwerp: Information-Sharing Network," February 2014, http://www.cbp.gov/sites/default/files/documents/bulletin_feb2014_antwerp.pdf.
[12] CyberKeel, "Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Sea," October 15, 2014, http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf.

requirement.[13] As a consequence, SCADA systems are often globally networked and, without sufficient security, can be compromised by cyber actors anywhere in the world.

In the maritime domain, these systems are part of a vast and complex port technology ecosystem; they collectively control vessels, cranes, vehicles, rail stations, storage yards, and loading docks—just to name a few. Whether the port is owner-operated or operated by one or more port operators, there are often many additional subsystems managed by companies who specialize in specific components. These are frequently outsourced to technology contractors, and as noted, sometimes without appropriate oversight of contractor performance and security by overarching stakeholders in the public sector.

U.S. Coast Guard officer Joseph Kramek wrote a 2013 study on cyber vulnerabilities in U.S. ports for the Brookings Institution, focusing on several priority-ranked ports based on their individual risk factors. Evaluating the Port of Baltimore, Maryland, he methodically follows maritime cargo from the ship through numerous technology-controlled automated processes to their next step in the intermodal system. He notes the automation begins instantly after docking, with computerized management software triggering notifications to networked cranes to unload containers. ICS-SCADA software orchestrates the entire process, telling crane operators where a container is to move next, and railcars and trucks when to expect the next container. Wireless networks are in extensive use, moving data into centralized databases while providing visibility to real-time data on cargo movements and equipment performance from SCADA systems, handheld devices, and other computers. Through all this technology, the port and intermodal operators are running at peak efficiency and incredible command-and-control of the whole process. Meanwhile, the port authority who leases the port to these contractors, has no meaningful visibility into the details of this complex technology ecosystem.[14]

The upside to all this infrastructure complexity is the rapid proliferation of automation, increasing the speed and efficiency of loading/unloading cargo and processing it through intermodal transfer for smooth, cost-effective distribution far beyond the borders of the port. On the other hand, more automation creates a hard reliance on potentially vulnerable ICS-SCADA systems, perhaps most alarmingly for the tasks mission-critical to operations—such as the crane functions and container tracking and movement.

Evaluating solely individual systems is at odds with the interconnectedness of critical infrastructure components. The growth of networked (and often Internet-connected) automation cannot operate at the scale necessary without critical dependencies on other sector's infrastructure. Electricity, in particular, may be the single most critical dependency of a port, and a vital factor in assessing where or to what extent port infrastructure is vulnerable. It is imperative that critical infrastructure systems be evaluated as part of an interconnected network with both individual and shared weaknesses that may not be obvious to, from, or on any one individual system.

---

[13] Bonnie Zhu, Anthony Joseph, and Shankar Sastry. "A Taxonomy of Cyber Attacks on SCADA Systems". University of California at Berkeley. http://bnrg.cs.berkeley.edu/~adj/publications/paper-files/ZhuJosephSastry_SCADA_Attack_Taxonomy_FinalV.pdf.

[14] Joseph Kramek, "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities", Brookings Institution, July 2013, https://www.brookings.edu/wp-content/uploads/2016/06/03-cyber-port-security-kramek.pdf.

Cross-Sector Dependencies

A Sandia National Labs technical paper notes the infrastructures creating the greatest number of dependencies are energy in all its forms, banking, telecommunications, and the full range of intermodal transportation infrastructures supporting maritime, rail, pipelines, roads, and air transportation.[15] Each of these sectors provides a piece of the assessment puzzle for understanding cyber risk in port infrastructure. As vital as each are independently and to each other, one sector in particular emerges as a particularly vulnerable dependency with the ports: electricity.

The importance of the energy sector to maintaining the security, stability, and operational continuity of ports and port operators is significant, and growing. On the one hand, the fragmentation of port operator's critical infrastructure and a legacy of manual operation means aggregate power usage trends of ports were not heavily researched prior to the last decade. On the other hand, studies are increasingly available, painting a clearer picture of both the tremendous energy consumption of ports, and how that energy is used throughout the port complex. A 2013 University of California, Los Angeles (UCLA) energy security study proved how difficult an undertaking this is. The UCLA study evaluated how power is generated, consumed, and used within the San Pedro, California area ports, including the Port of Los Angeles (POLA) and Port of Long Beach (POLB). Combined, these two ports form the busiest port complex in America and are routinely ranked among the busiest globally. However, as the study notes is true in San Pedro Bay, there is often not one centrally managed electrical system to contend with, but rather "many interconnected systems with hundreds of electricity billing meters, managed by multiple stakeholders with overlapping responsibilities."[16]

In POLA and POLB, energy costs likely exceed $50 million a year based on *individual* annual power consumption rates of approximately 183,000-233,000 Mega-watt hours. Container terminals alone—a centerpiece of port facilities and the broader intermodal system—were found responsible for half of that total consumption, bearing about $3 million a year in electricity usage fees. The majority of the remaining half were allocated to bulk terminals, and only 6-7% for port administrative facilities. The study concluded each of the two ports as individual entities would rank near the top of a small group of the very largest electric utility customers in Southern California.[17]

Predictably, the most automated systems and networks have the highest energy demands, marking a pivotal intersection of electricity and cyber vulnerability within the maritime domain. However, the reliance of ports on electricity is not limited to automated systems. It also includes the indoor and outdoor lighting necessary to maintain 24 hour functionality and security; the refrigeration/reefer systems required for the storage of goods throughout the intermodal transportation process; the wharf cranes used to lift and move containers; and others.

---

[15] Theresa Brown, "Dependency Indicators", Wiley Handbook of Science and Technology for Homeland Security, Sandia National Laboratories, http://www.sandia.gov/Fnisac/wp/wp-content/uploads/downloads/2012/03/Dependency-Indicators-article-w-figs.doc.

[16] Ryan Matulka, J.R. DeShazo, and Colleen Callahan, "Moving Towards Resiliency: An Assessment of the Costs and Benefits of Energy Security Investments for the San Pedro Bay Ports", UCLA Luskin Center, 2013, http://innovation.luskin.ucla.edu/sites/default/files/Port%20Report.pdf.

[17] ibid.

All of this power comes from an electric grid that already struggles to keep up with demand—routinely so, according to the UCLA study. Specifically problematic are "instantaneous frequency or voltage variations…not observable by commercial or residential customers…[that can] stop an array of wharf cranes as they unload a container ship."[18] Costing $75,000 in damages for the first hour the cranes are offline from one of these incidents[19], it is important to consider the economic impact of a similar scenario in a cyber context. If a nefarious cyber actor deployed malware through the electric power grid's SCADA systems to send frequency and voltage changes on demand, until that threat is identified and eliminated, they are in control. The consequences could last hours, even days, before systems are restored. Conceivably, malware-induced load spikes could overload both the power source and the many networks and systems connected to it. The economic fallout could spread quickly from one waypoint of the intermodal system to another; each dependent on the other, and the now-compromised electric power grid.

Backup power systems are available, and provide one form of contingency. However, beyond comparatively limited-capacity diesel generators designed for underway power and shore-side building- or facility-specific load demands, very few ports have any local power generation capabilities. The port's ability to maintain core functions at their nominal operating capacities is fairly limited. This makes port and operator facilities susceptible to the operational reliability and the cybersecurity of commercial or municipal power grids serving the port.

The grid is more than just an operational dependency. Power infrastructure and port infrastructure share many physical interconnections, and the presence of corresponding cyber interconnections is growing. As the power demands of ports continue to increase, more distribution lines, substations, and high-voltage substations are needed in order to effectively manage the flow of electricity to a port, and much of this is built on or immediately adjacent to the port property. Along with these linkages, there is a corresponding set of cyber infrastructure consisting of fiber cabling and wireless communication relays used to control these respective systems. The degree to which these systems are shared by the port operator and the power operator is not well established, but the proximity of systems would indicate that there are opportunities for shared vulnerabilities. Given some of the shared cyber architectures of their respective SCADA systems combined with the increase in their physical colocation, efforts should be made to examine their collective security from internal and external cyber threats.

All of this underscores why it is so critically important that port cybersecurity assessment models be more comprehensive than looking at when passwords were last changed or how many Microsoft Windows security patches have been installed. System-level assessments should be a vital part of an overall cyber risk mitigation strategy, but they are just one point in a deeply complex broader topology. Assessment models must not fixate solely on individual networks or systems. They must look at the combined networks and capabilities from end-to-end in order to identify otherwise relatively hidden dependencies. They must intentionally seek out vulnerabilities throughout that topology that, if exploited, could cause ripple effects far downstream into the individual systems in a port, or even upstream into geographically disbursed infrastructure that serves a much bigger area.

[18] ibid.
[19] ibid.

There is one additional factor worth considering with respect to the electric grid. An environmental regulation enacted in California and anticipated in all major U.S. ports in the near future will have a profound effect on port energy consumption. In turn, this may exacerbate these already troubling risks.

Upon arrival in a port, ships typically shut down their main engines, relying on their own diesel generators to keep their electrical systems powered. However, the exhaust created by diesel generators is responsible for a significant portion of the overall carbon emissions at a port. California's Environmental Protection Agency enacted the *"Airborne Toxic Control Measure for Auxiliary Diesel Engines Operated on Ocean-Going Vessels At-Berth in a California Port"*. The 2007 regulation's objective is the reduction of diesel particulate matter and nitrogen oxide emissions into the environment. In practical terms, it mandates a phasing-in of "cold ironing," or "shore power" to achieve those emissions reductions. This refers to the tethering of ships to land/grid-based power lines during parts of their time in port, or the generation of energy from alternative control technology that can achieve equivalent emission reductions. As a consequence, port power consumption is projected to double by the same 2020.[20] This regulation affects nearly every major port on the west coast of California and all their port operators, including those in Long Beach, Los Angeles, San Diego, Oakland, San Francisco, and Hueneme. Wholly 80% of docking ships in California will be required to use shore power by 2020.[21] While such regulations may provide a beneficial level of resilience through electric power redundancy in the event of a cyber-attack, capacity management should still be a significant concern. With the doubling of shore-side electric power consumption due to the new regulations, the trend couldn't be clearer: infrastructure dependence is only going to grow. A chief engineer at Southern California Edison told us they have to build out a lot of infrastructure in the ports to meet this projected demand curve. The capacity demands imposed on already vulnerable electric infrastructure raise our concerns about the survivability of the system in the event a potential cyber attack—particularly one that might aim to, say, remotely trigger voltage changes.

Power is not the only vital dependency for effective operations; the road and rail transportation networks extending out from ports are essential to move goods to and from the ships. Slightly more than 50% of imported goods are moved to their next stage of transportation by trucks, with the other half moving on a combination of on-dock, near-dock, and off-dock rail systems. When it comes to exports, 20% travel by rail, 30% by truck, and 50% by a combination of the two.[22] Each mode of transportation comes with specific cyber vulnerabilities, but they also share two critical overlapping IT systems: cargo manifests and container tracking.

The first system covers the process of tracking cargo through manifests. The manifests are now almost completely paperless and, as we saw in Antwerp, prone to relatively easy manipulation by cyber actors. Cargo manifests, provided by companies 24 hours in advance and aggregated by U.S. Customs at international ports, are vital to efficient operations and an accurate understanding of what cargo is

[20] Matulka and DeShazo.

[21] Air Resources Board, "Shore Power for Ocean-going Vessels", California Environmental Protection Agency, 24 Jun 2016, http://www.arb.ca.gov/ports/shorepower/shorepower.htm.

[22] Port of Long Beach, "Cargo movement in focus", 2008, http://www.polb.com/civica/filebank/blobdload.asp?BlobID=3512.

traveling through the system. The integrity of this data is essential for the security of the cargo itself, and each step of the intermodal transportation process.

The second system is known as "Virtual Container Yard", software for tracking and managing empty containers. It functions as a virtual clearing house for importers and exporters to dramatically reduce the number of truck trips needed just to exchange empty containers for future use. The loss of this efficiency, in place for more than 10 years, would have a profound effect on the operation of the port and is potentially vulnerable to cyber threats.

Ports already have a deeply intertwined dependence on other infrastructure systems to conduct port operations. Taking all factors in aggregate, this dependency will continue to increase. The ability of a port to mitigate risk and of public stakeholders to provide effective oversight of risk mitigation strategies cannot be limited to evaluating just the digital footprint of the port and its internal network of facilities and systems. It must also include the infrastructure the port is incapable of operating without; a cyber risk in one sector is highly likely to have a "spill over" effect in the other.

Economic & Operational Disruptions from Port Infrastructure Cyber-Attacks

Regardless of the cause, port closures or degradation of port operator's capacity can have a variety of negative effects, including economic losses. One port's failure may negatively affect connecting or nearby regional ports. These effects can be compounded on a global scale if no other regional ports have the equipment or capacity to handle the specific types of ships or loads transiting the impacted ports. This is often the case; ports are purposefully built to handle specific types of activity. Some, like Miami, Florida, are geared for large passenger vessels like cruise ships. The Port of Oakland, California, handles 99% of all container shipments in Northern California and ranks as one of the largest container ports in the nation[23]. Some ports are reasonably diversified: the San Diego area's five ports handle two cruise ship terminals and two cargo terminals[24]. Accordingly, a significant challenge is that if a cyber-attack degrades the capacity of an entire port or region, ships may not be able to simply sail to the next port up the coast and unload. The whole port complex must be able to handle the load, the additional capacity, and its throughput into the intermodal system.

Any decline in the operating capacity of a port can also generate potentially significant financial consequences. In 2002, an 11-day closure of 29 ports on the West Coast cost an estimated $11 billion— an incident that did not require reconstitution of any critical infrastructure. After 2005's Hurricane Katrina, maritime traffic up the Mississippi River came to a grinding halt for three weeks, backing up ships throughout the connected inland waterways. The estimated total cost of cleanup, reconstitution of infrastructure and operations, lost revenues, and other costs totaled an estimated $250 billion. Similarly, following Hurricane Sandy in 2012, Northeast ports lost an estimated $50 billion— suffering $1 billion in cargo delays alone. The United States is not alone in high-cost losses from degraded port operations. In 2011, the earthquake and tsunami that ravaged Japan shut down 15 major ports for two weeks, causing

[23] Port of Oakland, "Seaport", August 2016, http://www.portofoakland.com/port/seaport/.
[24] Port of San Diego, "Port of San Diego Overview", August 2016, https://www.portofsandiego.org/about-us.html.

a ripple effect that impacted shipping activity throughout the entire Pacific basin. World Bank cost-impact estimates ranged from $122 to $235 billion.[25]

To be fair, these numbers are not universally verifiable. Sometimes, stakeholders outside of the entity providing the estimate have no real way of verifying how it was calculated, how much revenue was simply deferred rather than lost and to what extent that hurts near-term finances, or whether parties have any incentives to inflate or minimize their estimates. However, what is certain is that shutdowns and disasters do have hard financial costs associated with them that can ripple across economically-interdependent industries. They also lead to the loss of confidence in the system, industry, or government's ability to respond and contain threats.

The dependence of most nations on maritime commerce also means the consequences of port interruptions may be potentially felt by millions who live nowhere near a port. Kramek's study concluded "the zero-inventory, just-in-time delivery system that sustains [port commerce] would grind to a halt…grocery stores and [gas stations] would run empty."[26] The cascading effects of a cyber-attack against maritime critical infrastructure may be far-ranging, from the economic fallout of product inventory sitting on ships unable to move to buyers, to breakdowns in energy distribution, to a consumer panic run on everything from daily necessities like household supplies to gas for vehicles. Kramek rightfully argues the cyber-induced consequences of a port shutdown in energy supplies alone are potentially cataclysmic, sending "shockwaves through the U.S. and even global economy.[27]"

This clearly illustrates physical or natural disaster impediments to port operations can impose catastrophic costs borne by governments, insurers, investors, and companies throughout the world.

From a cybersecurity risk standpoint, the cost-impact calculus is much more complex. The impact can—and should be expected to—transcend multiple port operators, critical infrastructure systems, and even sectors—spilling over from or between maritime, electric power, trains, trucking, and others in the intermodal transportation system.

As one example of this spill-over potential, a power outage to a distribution system feeding a port could have potentially crushing fiscal impacts. In December 2015, a cyber-attack against an electric distribution system in Ukraine caused an outage that lasted for eight hours, affecting between 60,000 and 200,000 people for varying periods of time. Using Ukraine and the 11-day closure of 29 West Coast ports costing $11 billion as a theoretical baseline, a similar outage at a major U.S. port could come in at a cost of more than $330 million to that port alone.

We can find examples of maritime/cross-sector cyber risk dependencies even in the U.S. space sector. In 2014, the United States Coast Guard (USCG) noted at a public meeting on maritime cybersecurity that a U.S. port suffered a breach that resulted in a seven-hour GPS signal disruption. The effect was a crippling of automated port crane operations. Without GPS data, the cranes were unable to establish their own positions, the positions of the containers they were supposed to move, and the locations to which those

[25] U.S. Department of Transportation, Research and Innovative Technology Administration, "ICS Security in Maritime Transportation: A White Paper Examining the Security and Resiliency of Critical Transportation Infrastructure," July 2013, pp. 6 - 7, http://ntl.bts.gov/lib/48000/48000/48074/DOT-VNTSC-MARAD-13-01.pdf.
[26] Kramek
[27] ibid.

containers were supposed to move to.[28] This kind of automation necessitates continuous access to accurate precision navigation and timing (PNT) signals from GPS satellite constellations. When access is hindered or accuracy degraded, automated operations cease to function. To the extent port operators have a contingency plan for operating on a manual basis, it may be possible to do so while automated operations are unavailable, but any such manual operations would be inefficient, time-consuming, and costly. Unfortunately, current maritime regulations do not mandate cybersecurity contingency plans that would address these kinds of scenarios.

Pointedly, this particular incident only affected four cranes. A larger or broadly-coordinated cyber-attack could have lasting consequences to a wide range of sectors and systems. The access vectors for these attacks need not be inside ports or port operators in order to achieve consequence in the maritime domain. In this example, a cyber-attack against the GPS satellites themselves, the networks that operate them, or the power sources supplying electricity for port and crane operation would all have a ripple effect that can reach down to the port operators and their equipment, docked ships, and others in the maritime space. Granted, some of those attack scenarios—such as a cyber-attack against the satellites themselves—are less likely given their universal usage would have far more global, catastrophic consequences on a humanitarian and security scale. However, the example serves to illustrate that assessing cyber risk or their potential cost implications in the maritime domain is not a simple function of imposing password complexity rules on end users or identifying SCADA or ICS systems connected to the public Internet with nothing more than a username and password to secure it from hackers. Maritime cyber risk assessments cannot be limited to end-user security policies or an evaluation of individual systems or even broader maritime networks. It must evaluate the co-dependencies those networks have with numerous other critical infrastructure sectors. It must review the contingency plans to which owners and operators will turn if their systems are directly or indirectly compromised. It must consider the extent to which security management is transparent to the range of public and private stakeholders who will bear just as much in gains or losses as the private companies who operate the infrastructure, or the insurers who back them. It must be a holistic, deep-dive assessment of how a port's or port operator's systems connect with each other and to/from outside entities, and a comparable assessment of the cyber vulnerabilities in those outside entities.

Port Infrastructure Cyber Attack Surface

Including the power grid and other critical infrastructure sectors in the cyber risk profile of a maritime environment means the potential cyber attack surface for port infrastructure is much larger. Troubling as that is, the reality is that a cyber-attack does not have to originate in a port system in order for port operations to be effected.

In order to accommodate the increasing demand for electricity from increased use of shore power, power companies are rapidly expanding their physical (and, by proxy, cyber) infrastructure located within ports. Requirements for specific substations and physical proximity to the ports are being added.

[28] Lily Hay Newman, "What if a Cybersecurity Attack Shut Down Our Ports?", Slate, May 2015, http://www.slate.com/articles/technology/future_tense/2015/05/maritime_cybersecurity_ports_are_unsecured.html.

While the heart of IT operations for power companies is typically located in their centralized control facilities, some operations technology systems like switches and digital relays will need to be installed along with the substations and physical infrastructure to handle the variable load requirements created by fluctuating demand at the port.

The ICS and SCADA systems utilized for electric grid operation and those used to operate port systems are not identical. While three SCADA software vendors comprise a majority of the systems found amongst electric operators, dozens of other vendors operate in maritime and other transportation sectors. There is no universal standard for how SCADA systems are to operate, or how they are to handle data transmission from field sensors through controllers all the way up to end-user SCADA terminals and into other sectors. However, there is enough similarity that infrastructure mapping of one sector is likely to provide some benefit to understanding and accessing the other. While there are no current examples of gaining access to a power company system and piggy-backing into a port or port operator's system, SCADA architecture similarities can potentially make that process easier.

While wireless connectivity at the ports can provide a path to hopping from port SCADA systems to their local power system, the move towards shore power comes with a potential new cyber risk in addition to the growth in energy dependency. The challenge is also the broadening of the potential cyber attack surface for effects against electric or port infrastructure. The cabling used by ships for the linkage are required to "accommodate fiber optic cable as part of the cable manager system located on the ship,"[29] with requirements for power synchronization but *undefined* requirements for IT linkage to the system. Cybersecurity protocols for docking ships will need to be established to ensure that breaches don't occur through docking ships accessing any of the port's systems. Even with protocols in place, the sheer quantity and variety of ships docking at major ports makes this attack vector more viable as a form of introducing malware or other malicious code into port IT systems.

Cyber Risk Prevention of Maritime Critical Infrastructure

While the structure and complexity of U.S. ports mean there are significant cybersecurity risks to the efficient and effective operation of the ports, there does exist a variety of governmental and private regulatory structures that are currently used to address physical security risks to U.S. ports. An analysis of these regulatory structures helps to inform potential approaches that may be utilized to address cybersecurity risks that pose a similarly significant threat to U.S. ports but have not yet been systematically mitigated through similar means. Analysis of the self-regulatory model utilized in the financial sector provides a model of an alternative regulatory structure that may be useful in shaping how cybersecurity risks are assessed in the maritime domain.

[29] Port of Long Beach, Engineering Division, "Shore to Ship Power Design Standard", http://www.polb.com/civica/filebank/blobdload.asp?BlobID=2158.

U.S. Regulation of Ports and Port Operations

The maritime domain in the United States is subject to a diverse patchwork of federal, state, and municipal regulations. At least eight federal entities have jurisdiction over some aspect of port operations: the Federal Maritime Commission, the U.S. Army Corps of Engineers, the Environmental Protection Agency (EPA), Maritime Administration (MARAD), the U.S. Coast Guard (USCG), U.S. Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), and the National Oceanographic and Atmospheric Administration (NOAA).[30,31] Port operators are additionally subject to state or municipal authority depending on the specific nature and history of the particular port.[32] Amidst this morass of regulation and operational oversight, the USCG, as part of DHS, is tasked with regulating and enforcing maritime port security.[33]

The USCG is broadly charged to "administer laws and promulgate and enforce regulations for the promotion of safety of life and property on and under the high seas and waters subject to the jurisdiction of the United States, covering all matters not specifically delegated by law to some other executive department."[34] It carries out this regulatory and enforcement role under a number of federal laws governing port security, including the Maritime Transportation Security Act of 2002 ("MTSA")[35] and the Security and Accountability For Every Port Act of 2006 ("SAFE Port Act", or just "SAFE").[36] Regulations issued by the USCG also seek to align (to the extent deemed appropriate by USCG authorities) with the two leading international treaties addressing port security issues: the International Convention for the Safety of Life at Sea, 1974 ("SOLAS", Chapter XI-2) and the International Code for the Security of Ships and of Port Facilities ("ISPS Code", or just "ISPS").[37]

MTSA and SAFE contain provisions directing DHS and the USCG to establish plans and procedures for the protection of the maritime domain.[38] These provisions are consistent with minimum requirements set forth in SOLAS and ISPS, but also establish additional requirements and systems that empower DHS and the USCG to take specific steps to enhance maritime security on a global scale. This includes provisions requiring the development of a national maritime security plan, systems of surveillance, crew identification programs, ship tracking capabilities, and a system for evaluating foreign ports. As part of these powers, the USCG reviews the security procedures of foreign ports and any vessel entering into a U.S. port. If the USCG is not satisfied with the sufficiency of those plans and procedures, they are empowered to take other security measures, including refusing entry to a vessel.

---

[30] Richard A. Lidinsky Jr. and Deborah A. Colson, "Federal Regulation of American Port Activities", Maryland Journal of International Law, Volume 7 | Issue 1 | Article 6, p. 50-55.
[31] D. C. Baldinelli, "The U.S. Coast Guard's Assignment to the Department of Homeland Security: Entering Uncharted Waters or Just a Course Correction?", 09 December 2002, https://www.uscg.mil/history/articles/Homeland_Security_Baldinelli.asp.
[32] Rexford B. Sherman, "Seaport Governance in the United States and Canada", Research and Information Services, American Association of Port Authorities, p. 3.
[33] Lidinsky and Colson, p. 53.
[34] 14 U.S.C. § 2.
[35] Pub.L. 107–295
[36] Pub.L. 109–347, 13 October 2006
[37] 33 C.F.R. §101.100;
[38] 46 U.S.C. Chapter 701.

The provisions of MTSA and the SAFE Port Act do not include specific standards that ports and vessels are required to meet. The MTSA and SAFE authorities do, however, empower the USCG to issue and enforce further requirements in the form of MARSEC Directives. MARSEC Directives are not public documents and are not publicly available due to the sensitive nature of their contents. When a new MARSEC Directive is issued, a public notice is published without specifying the requirements contained in the directive. Affected ports and vessels are then required to obtain a copy of the directive from their local Captain of the Port ("COTP"), a senior Coast Guard officer with response (including enforcement), prevention, and regulatory jurisdiction over a particular maritime area of responsibility. In order to obtain a MARSEC Directive from the COTP, affected ports and vessels are required to demonstrate that "that they are a person required…to restrict disclosure of and access to sensitive security information, and…they have a need to know sensitive security information" under applicable regulation.[39]

Under MTSA and SAFE, enforcement of MARSEC Directive requirements also falls to the COTP. [40] To carry out these enforcement powers, the COTP is authorized to exercise control and compliance measures consistent with the provisions of SOLAS, which include: (1) inspection of a vessel; (2) delay of a vessel; (3) detention of a vessel; (4) restriction of vessel operations; (5) denial of port entry; (6) expulsion from port; (7) restrictions on facility access; (8) conditions on facility operations; (9) suspension of facility operations; or (10) suspension or revocation of a security plan approved by the U.S., thereby making that vessel or facility ineligible to operate in, on, or under waters subject to the jurisdiction of the U.S.[41]

This existing regulatory and enforcement structure provides a robust framework for establishing a wide range of security standards applicable to vessels, ports, and port operators—including cybersecurity standards. Section 2, Title 14 of the U.S. Code charges the USCG to "administer laws and promulgate and enforce regulations for the promotion of safety of life and property on and under the high seas and waters subject to the jurisdiction of the United States, covering all matters not specifically delegated by law to some other executive department[.]"[42] Additionally, Section 70103 of Title 46 of the U.S. Code, which, among other things, establishes requirements for vessel and facility security plans, specifies that a required security plan should include provisions for "communication systems" and "other security systems."[43]

Accordingly, while existing laws, regulations, and MARSEC directives addressing vessel and facility security are primarily focused on physical security measures, the USCG would likely still be within its legal authority if it issued mandatory cybersecurity standards in the form of a MARSEC Directive. Coast Guard captains of the port have clear legal authorities for the prevention of and response to all hazards within their respective areas of maritime operations. Cyber transcends traditional domain/geographic borders and may cause effects across multiple jurisdictions, but a cyber-attack against port infrastructure will still be felt most acutely within the maritime domain entrusted to USCG and CBP authorities. Using this regulatory model to establish cybersecurity standards would have the added benefit of establishing a clear floor that would enable the COTP to enforce compliance if ports fail to implement a baseline of cybersecurity requirements.

[39] 33 CFR § 101.405(a)(2)
[40] 33 CFR §§ 101.105; 101.400.
[41] 33 C.F.R. § 101.410
[42] 14 USC § 2.
[43] 46 USC § 70103(c)(3)(C).

Classification Societies—A Public/Private Risk Management Model

In addition to the maritime security regulatory structure established under the MTSA and SAFE Port Act, there is a strong tradition in the maritime domain of establishing and enforcing operational and security standards through private means. "Classification Societies" have long played an important role in establishing seaworthiness standards, and those standards are often enforced within the international maritime community through the public insurance market.

Perhaps owing to its traditions as one of the most dangerous environments in the world, shared by all who sail, or perhaps to the diversity and complexity of stakeholders, the maritime domain is home to unique public/private models for managing risk that go well beyond statutory or regulatory structures codified by law or international treaties. This strong tradition of establishing operational and safety standards effectively balances public sector stakes with private sector ownership. Classification societies are self-regulating, independent, and externally audited. Their use dates back to the earliest days of shipping when insurers sought to evaluate the risk of particular vessels, crew, and goods transiting the ocean. These earliest efforts began in 1760 when maritime insurers at Lloyd's coffee house in London formulated a system of rules for the independent inspection of ships seeking insurance. The construction, safety, and operation of each ship and its equipment was "classified" according to a rating scale evaluating its seaworthiness or quality. Rating scales were grounded in a set of rules stipulating the technical standards insurers sought out in the design, construction, and safe operation of ships.[44] Combined with statutory regulations from international and country-specific laws, these collective requirements became the acknowledged global standard for ship safety, seaworthiness, and, later, pollution response. Today, dozens of classification societies exist around the world to conduct these inspections while ships are required to be evaluated during construction and periodic assessments thereafter.

This unique public/private model triangulates the needs of insurers, shipping companies, and governments; it has worked well for nearly all stakeholders as a risk prevention strategy. One of the lynchpins of the model is that, for understandable liability reasons, classification societies do not *guarantee* seaworthiness of a ship; their assessment evaluates whether the ship has met stakeholders' mutually agreed upon standards for ship design and safety. It is up to shipping companies and their crews to ensure compliance is maintained and ships operate responsibly in a safe and secure manner. Given private party ownership and control of ships—or, similarly, port infrastructure—this enables all stakeholders to have a clear rating as to the readiness of that ship to meet known threats to safety or security while private parties bear ultimate responsibility for the performance of their privately-owned resources.

Standards developed and adopted by classification societies, including significant participation from industry and other stakeholders, benefit from the real-world perspectives of those who are required to comply with the standards. It also avoids accidental regulatory overreach or over-prescriptiveness born out of an incomplete understanding of the full range of issues and circumstances faced by maritime

[44] International Association of Classification Societies, "Classification Societies: What, Why, and How?", http://www.iacs.org.uk/document/public/explained/Class_WhatWhy&How.PDF.

vessels, facilities, and operators. Additionally, standards developed by a classification society are more likely to be implemented on an international scale, as the private market for insurance and investment is not bound by the limits of legal jurisdiction.

On the other hand, compliance with standards from one ship to another can be highly variable because each individual classification society and the "flag" country of the vessel enforce standards differently. This variability is kept in check because, as private entities, a classification society stands to benefit financially if they maintain a consistent international reputation for strong standards, thoroughness, and technical credibility—and thus, in turn, shipping companies and other stakeholders stand to gain financially by doing business only with strong, thorough, and credible classification societies. However, the variability in class societies are driven in some part by virtue of being based in regions with comparatively lax laws and oversight. Countries can still individually choose whether or not to allow passage or entry of vessels into their ports that are from regions with standards they do not trust.

Another important aspect of the classification society model of assessment is that countries are authorized to designate leading classification societies as a "Recognized Security Organization" (RSO). Given the government staffing and funding challenges in meeting the sheer scale of compliance assessments needed, MTSA and ISPS allowed for approved RSOs to conduct the vessel security and facility reviews otherwise mandated of the USCG. Conclusions of RSO reviews carried the full weight of government as if it had done the assessments directly.

An Alternative Self-Regulatory Model from the Financial Sector

Classification societies and direct regulation by government agencies are the regulatory structures used today for setting and enforcing standards for the safety and security of vessels. In the U.S. financial sector, a potential approach can also be gleaned from the model of a Self-Regulatory Organization ("SRO"), offering a middle ground between direct regulatory enforcement of government and the complexities of cybersecurity that require different standards and enforcement means than an organization strictly defined by the classification society model.

SROs are private corporations with statutory authority to issue and enforce regulations. They are generally owned and financed by the entities and persons subject to regulation by the SRO itself. The most well-known SRO of this type is the Financial Industry Regulatory Authority ("FINRA"), which is authorized under U.S. securities law to exercise limited regulatory and enforcement powers over securities brokers and dealers under the supervision of the Securities and Exchange Commission (SEC).[45] Individuals and entities engaged in conduct regulated by FINRA are required to register for membership with FINRA in order to legally conduct business with consumers. In order to be accepted for membership, applicants must meet the requirements for membership established by FINRA, including in some cases passing exams testing applicants on applicable rules and concepts. The operations of FINRA are funded through membership fees of those required to register as members, with FINRA receiving no government funding. FINRA is empowered to establish rules and regulations regarding the conduct of its members and to impose fines and penalties for violations of its rules, including revoking the

[45] See 14 U.S.C. § 78-o.

membership of an entity or individual thereby banning the entity or individual from conducting business.

In the port environment, infrastructure capabilities and dependencies overlap numerous networks and technologies across multiple sectors. The interconnectedness and multi-domain nature of the environment means assessment bodies must have a broad range of extremely specialized technical skills in multiple domains. This kind of talent is both costly and incredibly hard to find. It also means an assessment body may be most effective when armed with the teeth of statutory enforcement powers while still subject to stringent certification requirements testing their capability to perform such a difficult job.

The model of an SRO, similar to that of FINRA, could, like classification society RSOs, be an attractive option for creating a maritime cybersecurity regulatory body that would combine the depth of knowledge and resources of a classification society or industry group, with the enforcement authority, mandatory participation, and independence of direct government regulation.

A Proposed Approach for Mitigating Cybersecurity Risk in U.S. Ports – Maritime Cybersecurity Assessment Organizations (MCAOs)

As discussed, U.S. ports face significant cybersecurity risks with the potential for far-reaching consequences and economic costs that would be borne by the public and a wide array of government and private sector stakeholders. Existing public and private regulatory models provide potential tools for addressing these risks. Some classification societies are in the early stages of evaluating cybersecurity risks of systems on board ships. However, the scope of classification responsibility typically starts and ends with the vessel itself. Shore-side, DHS "Cyber Security Advisors" are available upon request to provide cybersecurity advice, assessments, and incident support.[46] Similarly, mandated by Executive Order 13636, the Critical Infrastructure Cyber Community (C^3, or "C-cubed") offers a program for helping critical infrastructure operators implement NIST standards for cybersecurity resilience.[47] These programs are helpful starting points for shore-side seurity, but are ultimately voluntary and face extraordinary limitations on capacity. There are hundreds of ports alone in the U.S., let alone airports, power grids, water systems, and countless other critical infrastructure facilities; they get to only a small number of locations. These programs are also based on the NIST framework for cybersecurity, which is not domain-specific. Assessments are needed that incorporate the unique circumstances of each port's networks and location in order to effectively evaluate and mitigate cyber risk of shore-side maritime critical infrastructure, or its dependent systems within electric, transportation, and other sectors.

There are also other big challenges at play. Governments are ill-equipped and perennially under-funded to conduct such complex cybersecurity assessments on its own. They may have an overriding public interest in ensuring the security and continuity of such infrastructure, but if they lack the expertise or

[46] U.S. Department of Homeland Security, "Cyber Security Advisors", https://www.lfcc.edu/wp-content/uploads/2015/04/dhs-csa-fact-sheet-2014.pdf.
[47] U.S. Department of Homeland Security, "Critical Infrastructure Cyber Community Voluntary Program", https://www.us-cert.gov/ccubedvp.

the funds to recruit, train, and employ experts, the risk factors may not only persist, but grow as technology becomes increasingly more complex every year. In point of fact, the growth is not slowing and a Gartner report on cybersecurity beyond 2013 considers near-future cybersecurity to become "a perpetual arms race, between hackers and criminals on one side and enterprises and governments on the other side."[48]

This is a crucial argument to why an independent entity should work between public and private stakeholders to formulate port cybersecurity standards and conduct the deep-dive, multi-domain assessments. Government in general is not equipped to do this, and it is highly unlikely it will be able to in the near future. For 2016, the federal government estimated it would need to hire 10,000 cyber professionals just for current government cybersecurity programs[49], let alone for new ones in domains like maritime that remain vulnerable due to a lack of cyber oversight. The mountain government must climb is even higher when you look at the scope of what has to be done. The domestic U.S. maritime domain encompasses hundreds of ports stretching across tens of thousands of miles of shoreline, and assessments, as we've established, need to consider overlapping interests in sectors of otherwise unrelated expertise—like maritime and energy.

The disparity in pay scales between the private sector and public sector is also a significant factor. Experienced cybersecurity operators and analysts can command dramatically higher salaries from private companies. Top corporate cyber or IT executives can earn as much as three or four times what they would at the highest pay scales of federal agencies[50]. Short of an overhaul of the federal employment system, the most expeditious route to putting cybersecurity assessments in place in the ports is through an independent entity that can pay private sector wages, or close to it, while also ensuring the right combination of multi-domain expertise. Even if government was well-positioned to fill this mission-critical need, it will take many years to acquire the talent pool, train it, and deploy it as necessary. The threat is today, and the cyber-arms race is on the horizon.

Given the substantial challenges governments face in cybersecurity staffing, expertise, and ever-tightening budgets[51], a hybrid public-private model may offer a desirable middle ground that would offer the benefits of private regulation like classification societies with the enforceability of government regulation. Maritime industries thrive on stakeholder collaboration. There are unique sensitivities with cybersecurity that can expose error, fallibility, and security gaps within private companies—thus impacting stock prices, global revenues, and public perception. However, to the extent confidentiality can be protected through an independent entity, a public/private approach to assessing risk may also be the only way to overcome governmental gaps in cyber assessment capabilities.

---

[48] Mark Weatherford, "Government Must Attract More Cyber-Security Talent (Opinion)", Government Technology, 13 January 2010, http://www.govtech.com/pcio/Government-Must-Attract-More-Cyber-Security-Talent.html.
[49] Jack Moore, "Agencies Get Marching Orders for Filling 'Major' Cyber Talent Shortage", Nextgov, 15 December 2015, http://www.nextgov.com/cybersecurity/2015/12/agencies-get-marching-orders-filling-major-cyber-talent-shortage/124520/.
[50] Dan Verton, "The real cybersecurity workforce challenge: Hiring the 'best of the best' hackers", FedScoop, 18 June 2014, http://fedscoop.com/real-cybersecurity-workforce-challenge-hiring-best-best-hackers.
[51] Ronald Bailey, "Federal Cybersecurity: Not Even Good Enough for Government Work", Reason, 26 June 2015, http://reason.com/archives/2015/06/26/federal-cybersecurity-bad-enough-for-gov.

Under existing laws and regulations, we propose the creation of a Maritime Cyber Assessment Organization (MCAO) to address these gaps in national and international cybersecurity policy.

While we would argue the classification society model has worked well to balance conflicting public and private interests over ship design and safety for centuries, classification society influence largely stops at the edge of the ship. The risk mitigation needs of shore-side infrastructure demonstrate the need for a new type of entity; fast-moving, agile, and staffed to handle the intricacies of a multi-industry, multi-sector assessment. The MCAO model could be effectively employed, coupled with necessary cyber-specific authorities, to assess cybersecurity risk within the deeply intermingled infrastructure that extends well beyond the maritime domain on shore.

Like RSO classification societies and SROs in the U.S. financial sector, an MCAO would be a private corporation with limited statutory authority to enforce regulations related to cybersecurity compliance, resilience, and risk management. The USCG would have chartering authority to credential MCAOs for operation. U.S. ports and port operators would be required by Coast Guard regulations to be members of the MCAO in order to operate within the U.S. The MCAO would in turn be funded through membership, certification, and other fees charged to ports, port operators, or others in the maritime domain who wish to achieve a recognized standard of cybersecurity readiness.

As a private, non-profit corporation, the MCAO would operate under the supervision of the Department of Homeland Security and its appropriate agencies such as the U.S. Coast Guard, but be governed through an independent board of directors. The board of directors of the MCAO would be made up of representatives of both industry and government, as elected by MCAO members. Private full-time employees, operating independently of both industry and government under the supervision of the board of directors, would staff the MCAO's executive and operational teams.

Members of the MCAO, including all ports and port operators, could be subjected to MCAO-determined membership requirements, such as being required to meet certain minimum cybersecurity program and control requirements, and being subject to cybersecurity and IT exams by MCAO staff. Appropriately credentialed MCAO staff would conduct deep-dive, consultative cyber vulnerability assessments and testing of IT systems and networks within its member ports and operators, including cross-sector assessments for dependencies with (and vulnerabilities from) other critical infrastructure sectors such as power, rail, and trucking.

As a hybrid public-private, self-regulatory organization, MCAO cybersecurity standards, assessments, and ratings frameworks would be developed and implemented by MCAO staff in close coordination with maritime industry, government, and insurance stakeholders in ways similar to how classification societies established ship safety standards.

Independent and privately-financed, MCAOs would have the necessary flexibility and financial resources to hire and terminate as and when needed in accordance with normal private sector federal, state, and local employment laws. This independence also enables the flexibility to pay salaries commensurate with the private sector. This flexibility is absolutely crucial in an era where assessments require deep networking, protocol, software, and cyber intrusion expertise across multiple domains, and experienced cybersecurity and IT professionals easily command far more than government can pay.

In a departure from the financial SRO model, except for what is allowed by current rules, MCAOs would not possess enforcement authorities beyond lowering a port or operator's MCAO scoring, or revoking their membership; the latter effectively banning the entity or individual from conducting business until they can meet minimum standards. Instead, enforcement of MCAO credentials and cybersecurity requirements within the ports would fall under existing COTP authorities through MTSA, ISPS, and SOLAS control and compliance measures, and potentially shared authorities by other agencies that are beyond the scope of this paper.

In addition to establishing cybersecurity standards and conducting examinations, the MCAO would incentivize and actively enhance the cybersecurity of its members by offering cybersecurity support services. For example, as a sector-specific entity focused on cybersecurity with substantial expertise and cross-sector access, the MCAO would be in a uniquely ideal position to coordinate cybersecurity information sharing across its members and public stakeholders like law enforcement and intelligence personnel. This can ensure timely information is shared while still being sanitized of non-critical information not necessary for coordination and which if shared might expose private vulnerabilities or competitive intelligence. Additionally, the MCAO would maintain incident response and forensic teams with maritime infrastructure expertise to respond to cybersecurity incidents affecting its member entities. These teams would work extensively with USCG inspectors, investigators, and cyber protection teams throughout government. It would provide members with significant resources that would be difficult if not impossible to maintain individually. And in the event of a major cross-sector cybersecurity incident, the MCAO would be well-positioned to standup an Incident Command System unified response organization, staffed with cybersecurity experts to augment the incident response professionals in industry and government. By providing these additional services, the MCAO would offer significant value and support to U.S. ports and port operators in addition to enforcing a minimum standard of cybersecurity best practices.

Conclusion

The maritime domain is unique in its sheer size and in its complexity. Stakeholders throughout the world rely on the efficient flow of commercial goods and passage of ships in and out of ports; incidents that hinder or halt those operations have imposed enormous costs on industry, with a ripple effect felt by many, far away from the port. Its influence in global economics and security is matched only by the maritime sector's dependence on other sectors from electric power to transportation to keep it functioning and to keep goods moving smoothly from ship to shore to truck, train, or plane. Technology has enabled incredible operational efficiencies throughout this end-to-end intermodal system, by using extensive automated computer and networking systems.

The intersection of those systems and their physical and operational connections to systems in other sectors creates deeply interconnected infrastructure. Identifying cybersecurity vulnerabilities in the maritime domain is of paramount importance, but is greatly complicated by those inter-dependencies.

Current authorities and regulations in the maritime domain allow for setting and enforcing cybersecurity standards, but few exist. The lack of these standards combined with a pervasive lack of visibility by any

stakeholders into the details of the infrastructure in use in any given port is a critical national security gap. A policy and legal framework for how to assess cyber risk in this domain would go a long way to establishing an enforceable baseline for the government and private sector to guide their efforts with a common vernacular while still maintaining the flexibility to address the rapidly changing technology.

The challenge with government intervention begins with the fact that the vast majority of critical infrastructure is privately owned, operated, and paid for. This is exacerbated by government's inability to hire enough cybersecurity professionals across all international, federal, state, and local needs, and the top dollar commanded by experienced professionals in private industry. Industries in general are also reticent to embrace government regulatory intervention, but there are significant overriding national and international interests in making sure companies appropriately manage their infrastructure security.

Similar risks have been effectively mitigated for centuries. Classification societies have helped ensure strong ship design and safety standards by working as an intermediary between public and private stakeholders.

A similar approach must be embraced to reduce the threat of cyber vulnerabilities in ports. The most expedient and effective means of bridging all these gaps is a public/private partnership; an independent entity, funded and self-regulated by port members whose participation is mandated by regulation. This entity, a Maritime Cybersecurity Assessment Organization, would employ the private sector talent needed to develop considerable expertise in maritime critical infrastructure and its deeply rooted dependencies on the electric grid and infrastructure from other industries like trucking and rail. MCAOs would establish appropriate security standards between government and industry stakeholders, and in partnership with Coast Guard Captains of the Port, bear the regulatory authority to enforce those standards against non-compliant ports and port operators.

The model of a MCAO presents an attractive option for creating a maritime cybersecurity regulatory body that would combine the depth of knowledge and resources that are mission-critical to any meaningful cyber risk assessment, with the authority, mandatory participation, and independence of direct government regulation—without burdening government or corporate budgets with the astronomical costs of trying to do this all on their own. The creation of an MCAO would allow for a degree of coordination, communication, and the development of sector-specific knowledge and operational capabilities that would substantially mitigate cybersecurity risks facing U.S. ports and port operators, dramatically enhancing the safety and resilience of U.S. maritime critical infrastructure.