Maritime Cybersecurity: Meeting Threats to Globalization's Great Conveyor

Chris Bronk, Ph.D.
University of Houston
rcbronk@uh.edu

Paula deWitte, J.D., Ph.D.
Texas A&M University
paula.dewitte@tamu.edu

Abstract

This paper addresses the issue of cybersecurity in the global maritime system. The maritime system is a set of interconnected infrastructures that facilitates trade across major bodies of water. Covered here are the problem of protecting maritime traffic from attack as well as how cyberattacks change the equation for securing commercial shipping from attack on the high seas. The authors ask what cyberattack aimed at maritime targets – ships, ports, and other elements – looks like and what protections have been emplaced to counter the threat of cyberattack upon the maritime system.

1. Introduction

International maritime operations remain a primary vehicle of globalization. More than 80 percent of the world's cargo is carried by ship. While mobile phones and other small, lightweight, highly-valuable items may go by air, almost everything else traveling from continent-to-continent is transported by maritime vessels. Shipping remains a fundamental component to global trade, wherein ports large and small serve as the departure and arrival point for containerized, bulk, and liquid cargo.

Transport by ship has become a deeply automated process in which computers are employed in everything from navigation and propulsion to cargo handling and customs. Increasingly, the computers involved in maritime cargo operations are also networked, largely employing the same protocols as other Internet-based forms of communication [1]. This rise in networked computerization in ships and in systems that support shipping from onshore present new opportunities for malicious parties to disrupt maritime commerce in ways that piracy and open naval hostilities cannot.

Cyberattacks may be launched across global distances and can have potentially devastating impact. They can't necessarily be steered around as with threats like regional conflict or piracy. Nonetheless, we argue the threat of cyberattack is real and prompts us to answer several questions. First, we ask how does cyberattack threaten the global system of maritime enabled commerce? Second, we investigate the cyber threat to maritime system. In our third and last thrust of inquiry, we attempt to identify what norms, standards, practices, and law may be needed to protect the system of global maritime commerce from cyberattack as well as practical prescriptions for US public policy as well as international policy.

Before moving on to discussion of international security antecedents to cyber issues found in this area, there is a matter of definitional housekeeping. The authors prefer to use the term *maritime system* to define the operational space in which shipborne and port activities take place, principally for commercial purposes. US Coast Guard (USCG) and Department of Homeland Security (DHS) documents describe a Maritime Transport System (MTS) that encompasses much area where cybersecurity issues are to be found in the maritime system, but not necessarily all of it. DHS's definition extends to ports and coastal authorities but not necessarily ships plying the seas far from US territory.

For centuries, states have pursued control of the seas, often in competition or conflict with one another. While two great powers, the United Kingdom and the United States, have exerted much effort to control the seas and allow for the free flow of trade on the world's oceans, other powers have contested their (mostly) benevolent hegemony for the seas [2]. Ahistorical perspectives on maritime security are likely foolish while thinking about cybersecurity issues as cyberattacks may well achieve results previously ascribed to warships, privateers, or pirates on the high seas.

2. Seaborne Commerce and Sea Control: Lessons from the Last Century

URI: https://hdl.handle.net/10125/63979
978-0-9981331-3-3

Disruption of shipping activity is often fundamental component of naval conflict [3]. In both world wars, submarine campaigns represented a mortal threat to multiple powers, but not least the island nations of the Axis and Allied coalitions. In the Second World War, it could be argued that one submarine campaign, Germany's in the Atlantic, ultimately failed, though at great cost to the Allies, while another, the United States' campaign against Japanese merchant shipping, was a success. For decades after the war, the United States and its NATO allies prepared for a clash of naval forces and doctrine in the North Atlantic.

There the issue was to what degree NATO's naval forces – surface ships, submarines, and aircraft – could protect a massive reinforcement from North America to Europe. It was assumed that the Soviet Union would sortie hundreds of submarines and surface warships to disrupt the Alliance's maritime link. How well the respective strategies of NATO and the Soviet Union would have fared remains a well-educated guess, but few estimates were particularly rosy with regard to the fortunes of merchantmen on the North Atlantic in a potential war with the Soviet Union [4]. Nonetheless, in 1986 Mearsheimer argued, "the Navy's main value for deterrence lies in the realm of sea control, where protection of NATO's sea lines of communication (SLOCs) might matter to Soviet decision-makers contemplating war in Europe" [5]

While no major war between East and West came to pass between 1945 and 1989, regional conflicts did have an impact on international maritime commerce. Perhaps most important of them was the closure of the Suez Canal from 1967 to 1975. Shut at the onset of the June 1967 Six Day War, Israeli and Egyptian troops faced off across the 120 mile-long waterway between the Mediterranean and Red Seas until 1973's Three Day War. The canal was ultimately reopened as relations improved between Cairo and Tel Aviv in 1975. The canal's closure increased the distance of a sea journey from Mumbai to London from 6,200 nautical miles to more than 10,800 nm. Feyrer argues persuasively how closure of Suez led to significant reduction in trade between nations on either side of it [6, 7].

Despite being the last naval conflict of its kind, the 1982 War over the Falkland Islands had minimal impact on international seaborne commerce, during the war between Iran and Iraq from 1980 to 1988 merchant ships involved in the export of oil from both belligerents were attacked more 450 times [8]. Both sides sought to interdict their opponent's capacity to sell oil internationally thereby acquiring funds to continue the war effort. US intervention in the Persian Gulf during the conflict ultimately led to the crippling of two warships, the *Stark* (hit by Iraqi missiles) and *Samuel B. Roberts* (which struck an Iranian mine). US protection of commercial shipping illustrated that such duty remained dangerous and unpredictable, however punitive attacks on Iranian forces after the damaging of the *Roberts* largely curtailed Iran's capacity to harm US or allied commercial vessels.

Absent major international conflict, disruption to maritime commerce has arisen in new forms. Somalia's incapacity to exert control over her littorals during the country's slide to largely ungoverned status in the 1990s led to a resurgence in maritime piracy in the 2000s. Regional warlords and bandits engaged in a significant piracy campaign, involving the hijacking of dozens of vessels, some held for periods of years for ransoms in excess of $1 million. However, coordinated international response as well as military operations onshore have had a desired result of reducing the Somali pirate problem to a negligible one [9].

3. Cybersecurity and the Maritime System

When we think of piracy on the high seas, it is a mostly unsophisticated endeavor. A few men, armed with rocket propelled grenades and Kalashnikovs, possessing boarding gear and a fast boat are usually all that is needed to highjack a vessel displacing 50,000 tons or more (naval vessels excepted). Ransoms for these hijacked ships has reached well into the millions of dollars.

How cyberattack may disrupt shipping is different. To get our arms around cyber threats, we need to begin using some imagination as to what is requisite for a pulling off a cyberattack that either steals something of value or does damage to a maritime vessel or other piece of infrastructure. The authors like to consider the beginning point of thinking about such attacks as the *bad guy-ology* of the attacker.

What does this mean? When we speak of bad guys in cyberspace, we are talking about people who can act alone, in small groups or large ones, supported or deployed by nation states or not. They craft source code for sophisticated tooling, penetrate computer networks, and do a lot of the same data management work as most Internet enterprises (servers, databases, means of communication, etc.) also toil in [10].

We have witnessed reports of computer security breakdown in the face of increasingly sophisticated

attack for more than 20 years now. This has been going on for a long time. Hackers and, equally importantly, hacker groups have been around for a while and they have evolved within both domestic and international political spheres. They have power. A former member of the Cult of the Dead Cow (cDc) hacker organization ran a Democratic campaign for one Texas's US Senate seats in 2018.

Concurrently, there has been a convergence of politics and cyberattack that extends from "kinetic" hacks like the *Stuxnet* campaign launched against Iran's nuclear enrichment program and the information warfare operation exemplified by the email breach at the US Democratic National Committee by foreign, state-supported hackers. Those individuals, in the employ of Russia leaked stolen data to the Wikileaks organization during the 2016 US Presidential election. Both these episodes illustrate how important or impactful cyberattacks have been and what breaks when they occur.

Thus when we begin thinking about cyber vulnerabilities in the maritime sector, we need to focus firstly on what happens when things break [11]. There is an exercise afoot in which mapping vulnerabilities to components are linked to pieces of information and computing infrastructure. We may not need to worry about a pump that can only be turned on by a human being, but one operated by computer and interconnected by network, we do worry about.

Where cybersecurity concerns come into play is after identifying things that could go wrong, i.e. that also are very detrimental to safety or continuation of operation. There need to be many people thinking about what can go wrong in shipping as with any piece of critical infrastructure. It may seem simple, but the computerization of it is not.

Furthermore, it must be reminded just how important maritime trade is to the global economy and what disruptions to it may produce in global manufacturing or energy supply chains. Hopefully this answers the question of why cybersecurity in the maritime system is important. It's important because of how closely seaborne trade tracks with world GDP and other economic indicators. Trade on the oceans exceeds 10 billion tons per year [12]. With many nations highly dependent on forms of import or export, disruption of those flows could be potentially useful to adversaries or enemies. In a time of increased economic conflict, could the cyber weapon not be employed against the maritime system? Of course, and it already has.

The *Stuxnet* or *Shamoon* of the maritime system, thus far is the cyberattack against Denmark's Møller-Maersk, the world's largest container ship operator. But Maersk is not just the biggest in container shipping, it also operates the ports themselves, including the Port of Los Angeles, the busiest port by container volume in the US. Maersk was also the victim of the most expensive and destructive cyberattack against any form of logistics company in June 2017.

The company's IT infrastructure was walloped by the propagation of the *NotPetya* malware across its computer networks. It was crippled by the attack, which shut down port operations – cranes, gates, freight forwarding instructions, and many, many other processes, at 17 of the company's 76 ports. After the attack, "For days to come, one of the world's most complex and interconnected distributed machines, underpinning the circulatory system of the global economy itself, would remain broken" [13].

With Maersk's woes as a backdrop, thinking about the bad guy-ology of cyberattack in the maritime system is shaped by two avenues for action. First is beginning with a desired impact of an attack, perhaps misidentifying cargo containers to facilitate smuggling. The second relates to systems' exposure to attack and how vulnerabilities may be exploited to produce a desired effect. So, we can start with two general types of questions. One is, "If I want to disrupt *x* with some form of cyberattack, how do I do it?" But also important is, "If I can see a vulnerability on resource *y*, what can I do with it?"

Returning to the Maersk case, it has been largely judged to be a victim of a cyberattack spilling over from the years' long conflict between Russia and her former sister republic, Ukraine. So the enormously costly attack on Maersk was the collateral damage of a Russian-sponsored attack on a country more than 1,500 kilometers from Maersk's headquarters in Copenhagen. So for as much damage and distress as *NotPetya* visited upon Maersk, it wasn't the intended target. We are left to wonder what damage an attack with some intent and planning might do to another major shipper and operator of ports.

Moving forward, we need to chronicle the places in which bad things can happen by cyber means and categorize them to some degree. The apparent dichotomy for maritime cybersecurity is a divide between operations at sea and those undertaken while in port. This is a useful distinction as the level of data connectivity for ships at sea is far more constrained than for other pieces of the maritime system functioning at pier-side and further inland. While ports and their IT infrastructure largely benefit from connectivity to high-speed, backbone Internet networks, ships at sea do not. They rely almost exclusively on satellite connectivity to transmit and receive data, and that connectivity is vastly

expensive. But let us begin with the cyber issues faced by ships at sea.

3.1 Cyber Issues for Maritime Vessels

Navigation by stars and sextant has been largely abandoned by the world's mariners. Most ships ply the world's sea lanes with the aid of three computer-driven systems: the automatic identification system (AIS); the global positioning system (GPS); and the Electronic Chart Display Information System (ECDIS). These three systems are the pillars of computerized navigation for merchant shipping today.

"AIS is a non-encrypted transponder responsible for transmitting course, speed, type of vessel, type of cargo, at-anchor or underway status; and other information for safety at sea" [14]. AIS transponders have been required of ocean-going vessels since 2002, however the functionality of AIS has been subverted for a variety of purposes. Substantial evidence exists that Iran switches off AIS transponders to facilitate sanctions evading behavior in its export of crude oil. North Korea also allegedly disables AIS ostensibly to allow its merchant vessels a greater degree of latitude in avoiding sanctions.

Also important to maritime navigation is GPS. Its use makes navigation on the high seas far more accurate and simple than ever before. As long as a merchant vessel can communicate with satellites of GPS system, its location can usually be pinpointed within a few meters. GPS is also employed in military targeting, and as a result, measures able to confuse, block, or spoof GPS signals have appeared. The US Coast Guard issued an alert regarding a 2015 incident in which a loss of GPS connectivity to multiple ships departing a non-US port occurred. In 2017, multiple vessels observed degradation and loss of GPS connectivity while sailing in the Black Sea.

Of all the systems of concern with regard to cyberattack, perhaps none is more worrisome than ECDIS. As it is a system that interfaces with navigational gear, sensors, and control systems for driving the ship, ECDIS represents a highly-dangerous target to cyberattack. Even bad ECDIS data is a significant issue. The US Navy minesweeper *Guardian* was severely grounded off the Philippines in 2013 largely due because, "leadership and watch teams relied primarily on an inaccurate Digital Nautical Chart (DNC) coastal chart during planning and execution of the navigation plan" [15]. In addition, multiple cybersecurity and maritime publications have reported on ECDIS's susceptibility to manipulation by unauthorized parties, possibly leading to grounding or collision.

In addition to the major navigational systems present aboard contemporary merchant vessels, there is an enormous amount of automation in shipboard operations. Contemporary cargo vessels, including the largest ones, have automated away large numbers of crew. Large merchant vessels displacing upwards of 100,000 tons are now operated by crews as small as 10 persons or less. The computer systems that replace crew members are process control systems, often provided by automation firms servicing multiple sectors.

One of them is Schneider Electric, a French firm that offers products in no less than 11 merchant shipping applications. Schneider's products are germane to this paper as its Triconex® brand of process control software is widely-utilized in industrial applications in a variety of sectors. Unfortunately, it was also allegedly compromised by a cyberattack in a petrochemical facility in Saudi Arabia. Shipboard systems likely contain a significant number of vulnerabilities, and while they can't be attacked in the way cable- and fiber-based networks are, there are plenty of other avenues for attack, including by insiders in a constant churn of crew turnover.

3.2 Cyber Issues in Port Operations

While ships at sea present a peculiar case in what may be considered operational technology (OT) cybersecurity, operations on land are quite different. While shipboard systems may largely be disconnected while at sea, port systems are largely interconnected and often widely exposed to the Internet. And what complicates their cybersecurity even more is that ports are incredibly heterogenous in ownership, operational, and technological composition. Coast Guard port inspectors reputedly quip, "If you've seen one port, you've seen a port."

Ports are often owned by local or regional governments, operated by a commercial operators, and served by myriad firms and offices who make the port work. Consider the Port of Houston, one of the nation's largest, and the most energy-related port in the United States (more on that later). Along the 52-mile Houston Ship Channel is the Port of Houston and its Port Authority (PHA), a mix of publicly- and privately-operated shipping terminals, and other port facilities, 150 different ones in total. It is home to the second and third largest oil refineries in the US and considered the primary energy port in the country. Some 260 million short tons of cargo and more than two million twenty-foot equivalent cargo containers passed through it in 2018.

It is also a very highly automated and networked port. And at the core of the digital operations is something called Navis. Navis is an interconnected suite of software;

> [D]esigned to manage all facets of terminal and cargo operations; it employs, among other things, optical character recognition to scan cargo and manage its movement. When cargo exits the port by truck or rail, not only does NAVIS [sic] electronically log the cargo out and thus simultaneously functioning as part of PHA's security access control system, it also generates billing invoices for PHA. PHA's gantry cranes, fuel farms, and even its HVAC systems are networked [16].

Thinking like a good bad guy, if so much of the Port of Houston's daily operations are largely dependent on the Navis software, then that is probably also an excellent target if the aim is to steal from or disrupt the port. Has Navis been compromised or been found vulnerable? Yes, in 2016, a SQL-injection flaw (a vulnerability found in a database service) was found in Navis software. The US Department of Homeland Security's now defunct Industrial Control Systems–Computer Emergency Response Team (ICS-CERT) reported a previously unknown vulnerability and Navis released a patch for it. The vulnerability could have been exploited by a novice attacker [Q].

Navis has published a library of white papers on enhancing port efficiency. They have titles like *A New Frontier: Business Intelligence, Big Data & the Impact on the Global Supply Chain* and *Port of the Future: A Sense of Wonder*. None of its white papers cover the topic of cybersecurity.

Although Navis and other port system software may have a central role in operations, the systems of many companies and government agencies also interconnect at major ports like Houston. These organizations run email systems, web servers, databases, and all manner of OT systems having to do with port operations. Some of the firms participating in port operations are among the largest corporations or conglomerates in the world, but others are far smaller.

What this means is that getting all the actors involved in the operation of a large US cargo port to adopt a framework or set of practices regarding cybersecurity is difficult. As the Maersk cyberattack illustrated, the loss of even one major firm's system at a large port may bring operations to a screeching halt. Of course there are many things that may occur to disrupt port operations.

Again, port cybersecurity is different than ship cybersecurity. The targets aboard ships that bad guys care most about are likely those related to navigation and propulsion, both highly automated in contemporary merchant vessels. But in ports, there are many more points of entry to interconnected port systems. Modern port systems talk to railroad systems, and Navis has software, "to automatically route railcars to hub assignments and plan train load sequences" [17].

What this amounts to is a scenario in which the purveyors of port operations computer software and automation drive to enhance interoperability and operational efficiency as their primary activity. This drive for efficiency is acceptable, however, automation rife with cyber vulnerabilities may be exploited by malicious actors. Such exploits must be countered by law, policy, and technology. How government and the private sector cooperate on preventing cyberattack is critical to the ongoing function of the global maritime system.

4. Law, the Sea, and Cyberspace

A fundamental issue pertaining to the law in sea is the concept of jurisdiction or the *power of a court or locale to regulate persons, objects, or conduct under their law*. Because the world's oceans are international, there is an issue of who has jurisdiction in matters occurring on the oceans. The United Nations Law of the Sea Convention (UNCLOS) attempts to establish a legal framework for the peaceful, cooperative use of the seas. UNCLOS replaced other UN initiatives with this framework. UNCLOS binds only those member countries of the UN and establishes jurisdiction for each country as 12 nautical miles (13.8 miles) from the coastline with a 200-mile exclusive economic zones.

However, multiple countries claim jurisdiction based on their own laws. United States Law, for example, claims that the:

> Special territorial and maritime jurisdiction of the United States includes: (1) The high seas, any other waters within the admiralty and maritime jurisdiction of the United States and out of the jurisdiction of any particular State, and any vessel belonging in whole or in part to the United States or any citizen thereof, or to any corporation created by or under the laws of the United States or of any State, Territory, District, or possession thereof, when such vessel is within the admiralty and maritime jurisdiction of the United States and out of the jurisdiction of any particular state. [19]

The issue of jurisdiction is especially problematic when it comes to cyberattacks. Does jurisdiction refer to the originating nation of the

attacker? The nation of the target? What is a nation is used as an intermediary in the attack? Can multiple nations claim jurisdictions? Unfortunately, the current status of the law remains fragmented with attempts to re-use existing laws and regulations into cyber attack scenarios the challenges to our current civil law framework and in more particular our maritime law legal framework center upon the application of existing legal concepts. This general lack of jurisdiction over hackers presents another issue. What if the damage from the cyberattack is not physical and the lack of physical damage arising from a successful Information Technology (IT) environment cyberattack are legal issues difficult to place within our current civil law framework. In short, the lack of physicality in an IT environment cyberattack presents challenges to our existing civil law framework.

Another attempt to regulate internationally is with the Tallinn 2.0 Manual for International Law Regarding Cyber Operations [20]. The title of this document is problematic. First, it is not international law but rather an attempt by NATO to define rules regarding cyber operations binding among NATO countries. Secondly, the term "cyber operations" is misleading as, on its face, it seems to mean transactions related to cyberspace, but in reality is synonymous with cyberwar.

The Tallinn Manual establishes a basis for sovereignty, due diligence, jurisdiction, and international responsibility and these uses this basis to prescribe laws for air, sea, and space. Its chapter on the Law of the Sea promulgating ten rules based on the recognized 200-mile economic zone. Both the Tallinn Manual and UNCLOS are limited based on their ability to control the members of their respective groups. As cyberattacks become more common against maritime assets, it will be up to the international courts to determine the effect of regulations and laws, and if these courts actually have the power to regulate.

5. Relevant Public Policy

As mentioned above, protection of the maritime system in the wake of the September 11 attacks on the United States and elsewhere has largely been aimed at protecting the physical security and integrity of cargo operations. Planning in port and shipboard security has largely been aimed at thwarting terror threats (smuggling of nuclear weapon or radiological components, other weapons, piracy, etc.) not cyber ones. That said, cybersecurity, or at least cybersecurity risk management has received attention from US national policymaking bodies as well as international organizations and associations.

5.1 US Cyber Security Policy Guidance

In the United States, there are sixteen critical infrastructure sectors. These sectors cover cyber as well as physical security. The cybersecurity of ships and ports falls under the DHS's Transportation Systems Sector (TSS). That sector covers not only maritime issues, but also highways, rail, aviation, pipelines, and postal operations. The TSS plan was released by DHS in 2015. It covers a great number of industries, and identifies the Coast Guard as the lead agency for maritime safety and security, including cybersecurity. This status is the point of origin cybersecurity strategy produced by the USCG. In addition, the US Maritime Administration (MARAD) maintains an Office of Maritime Security which has added cybersecurity to its portfolio.

Establishing the path for securing systems relevant to maritime operations from cyberattack has become a priority in the US. US policy on cybersecurity for the MTS is still developing, but was outlined in the *US Coast Guard Cyber Strategy*. The strategy rests on three pillars: defending cyberspace; enabling operations; and protecting infrastructure. That final piece is where the Coast Guard places the MTS mission, stating:

> Maritime critical infrastructure and the MTS are vital to our economy, national security, and national defense. The MTS includes ocean carriers, coastwise shipping along our shores, the Western rivers and Great Lakes, and the nation's ports and terminals. Cyber systems enable the MTS to operate with unprecedented speed and efficiency. Those same cyber systems also create potential vulnerabilities. as the maritime transportation Sector Specific agency (as defined by the national infrastructure protection plan), the Coast Guard must lead the unity of effort required to protect maritime critical infrastructure from attacks, accidents, and disasters [21].

The US Coast Guard's strategy heavily emphasizes risk management. This makes a great deal of sense, as shippers and other operators in the maritime system have a long history of managing risk and employing insurances to mitigate risk of loss (UK insurer Lloyd's has been in operation since 1686).

The Coast Guard's strategy rests on two legs: (1) assessment of risk through promotion of cyber risk awareness and management; and (2) prevention via the reduction of vulnerabilities in the MTS. This strategy is likely in need of revision, it was released

in 2015, and it's concrete objectives – risk assessment tools and methodologies; cybersecurity information sharing; cyber vulnerability reduction; and cybersecurity education and training – align with the early stage of cybersecurity development found in the maritime system.

5.2 International Cybersecurity Guidance

Beyond US policy, the International Maritime Organization (IMO) also has begun to stir in approaching the issue of how cybersecurity impacts its role at the UN specialized agency concerned with, "the global standard-setting authority for the safety, security and environmental performance of international shipping." The IMO issued guidance on maritime cyber risk management in 2017 [22]. It detailed eight areas of where vulnerable systems can be found, including:

- Bridge systems;
- Cargo handling and management systems;
- Propulsion and machinery management and power control systems;
- Access control systems;
- Passenger servicing and management systems;
- Passenger facing public networks;
- Administrative and crew welfare systems; and
- Communication systems.

The IMO's primary tools for guidance emanate from other bodies including: The *Guidelines on Cyber Security Onboard Ships*; the International Organization for Standardization and International Electrotechnical Commission ISO/IEC 27001 standard on security techniques; and the US National Institute for Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*. While the latter two documents are applied broadly to many areas of commercial activity, the Guidelines on Cyber Security Onboard Ships (GCSOS) is a much more specific one and deserves greater attention.

Where the USCG has hung its hat on a strategy for cybersecurity in the MTS, GCSOS is an attempt to move toward an industry guidebook for securing shipboard systems. Therefore it draws significant attention on a set of initiatives that can protect maritime activity. It represents the combined work of nine major associations involved in maritime shipping and transport. Furthermore it is focused on the cybersecurity of ships, *not ports*.

The GCSOS is a seven part document that may be best described as a handbook on cybersecurity related to ships engaged in commercial activity. It identifies the primary concern regarding cybersecurity to be found in this area:

> As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet.

The document also identifies the two major areas of concern regarding a cyberattack upon a ship; its navigation and propulsion systems. Without those functioning properly, safe shipboard operations can't be guaranteed [23].

Because the GCSOS is essentially a handbook or perhaps even a primer, it covers the full gamut of cybersecurity issues from threats to response and recovery in a relatively brief document. Nonetheless, it stands as significant contribution to cybersecurity in the maritime system. Moving beyond the primer phase of cybersecurity in the maritime system will necessitate new approaches and investments, detailed in the final section of this paper.

6. Conclusion and Prescriptions

Maritime cybersecurity has been identified as an issue of some importance in the global cybersecurity agenda. It does not rank as high as energy or power issues, nor have the maturity of corporate and government response found in the financial sector, but it is on the agenda.

We see the state of maritime cybersecurity as this. There is some emphasis on ships, but less on ports, and less still on things connected to ports. All matter and with many, many points of connection to port systems, establishing international, industry-wide standards will likely require extensive coordination and expenditure of intellect. Nonetheless, activity can be undertaken to secure the maritime system by policy and through educational endeavor.

6.1 Directions for Public Policy

Obviously maritime cybersecurity issues are inherently international or global in nature. Their remedy will require an investment by stakeholders in both government and the maritime industry with significant input from players in shipbuilding, maritime operations, port activities, and other functions that may be found in the maritime system.

If mere regulation was the answer to cybersecurity issues in this area of endeavor or any other, the job would be one from policymakers alone. Regulation will be only a part of the process of

increasing cybersecurity capacity. Nonetheless, when useful frameworks, guidance, rules, and international law may be promulgated, they should be. We just need to be cognizant of the rapid change that may occur as a result of technological innovation. It may be difficult to forecast the future vulnerabilities produced, but certainly this does not constitute a pass for policy action.

Policymakers concerned with addressing the cybersecurity issues to be found in the maritime system must recognize that a workforce of experts in cybersecurity able to address the issues faced by shipping lines, naval architects, automation software developers, or port operators will need to be created and grown. Its beginnings will stem from the tiniest of cadres now extant.

The maritime cybersecurity workforce will be composed of professionals who understand the programming and operation of computer systems as well as having an understanding of the multiple areas of expertise found across the maritime system. For instance, addressing issues in ship propulsion systems requires skills in both the operations of those systems as well as the cybersecurity problems that arise in their development and operation. The same would be true of systems for tracking cargo or navigation.

6.2 Research and Education

The workforce issue will necessitate training and education of varying depths. Some professionals will no doubt receive cybersecurity education and training at mid-career while others, if demand is sufficient, will enter the workforce with specialist degrees combining maritime and cybersecurity curriculum. At a deeper level, experts from industry, government, and academia may well need to collaborate around centers for interchange of expertise and research activity. This is already present in cyber activities for everything from the power grid to the banking system.

In the United States, a maritime cybersecurity research and development capability should be established along the lines of Department of Energy (DOE) cybersecurity organizations across its infrastructure of national labs. Considerable investment has been undertaken by the DOE in cybersecurity for the electricity power grid as well as other process control systems. DOE has made considerable investment at its Idaho National Lab (INL) in cybersecurity for Supervisory Control and Data Acquisition (SCADA) systems, found in all manner of industrial applications.

Both DHS and MARAD have grants programs in place for enhancing security of the MTS and ports. One official with whom we discussed this paper described one of the DHS program's outcomes being multiple sales of updated fireboats to major ports. This was verified in our research of DHS granting activity. How government funding can be coupled with industry initiatives should be another area for activity in the cybersecurity of the maritime system.

Few areas of critical infrastructure are more ripe for strategy and investment related to cybersecurity protection than the maritime system. In addition, research should be undertaken on the protection of computer systems in both shipboard and port operations so that cyberattacks will be less damaging or debilitating to maritime trade.

References

[1] Øvergård, Kjell I., et al. "Critical incidents during dynamic positioning: operators' situation awareness and decision-making in maritime operations." *Theoretical Issues in Ergonomics Science* 16.4 (2015): 366-387.

[2] Bueger, Christian. "What is maritime security?." *Marine Policy* 53 (2015): 159-164.

[3] Mahan, Alfred Thayer. *The influence of sea power upon history, 1660-1783*. Read Books Ltd, 2013.

[4] Wood, Robert S., and John T. Hanley. "The Maritime Role in the North Atlantic." *Naval War College Review* 38, no. 6 (1985): 5-18.

[5] Mearsheimer, John J. "A Strategic Misstep: The Maritime Strategy and Deterrence in Europe." *International Security* 11, no. 2 (1986): 3-57.

[6] Feyrer, James. *Distance, trade, and income-the 1967 to 1975 closing of the Suez Canal as a natural experiment*. No. w15557. National Bureau of Economic Research, 2009.

[7] Parinduri, Rasyad. "Growth volatility and trade: evidence from the 1967-1975 closure of the Suez Canal." (2012).

[8] O'Rourke, Ronald. "The Tanker War." *Proceedings*, Vol. 114 No.5, May 1988.

[9] Murphy, Martin N. *Small boats, weak states, dirty money: the challenge of piracy*. New York: Columbia University Press, 2009.

[10] Coleman, Gabriella. *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso books, 2014.

[11] Nicholson, Andrew, et al. "SCADA security in the light of Cyber-Warfare." *Computers & Security* 31.4 (2012): 418-436.

[12] Review of Maritime Transport, United Nations Conference on Trade and Development, Geneva, 2017.

[13] Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*. August 22, 2018.

[14] Hayes, Christopher R. *Maritime cybersecurity: the future of national security*. Diss. Monterey, California: Naval Postgraduate School, 2016.

[15] Command Investigation into the Grounding of USS Guardian. United States Pacific Fleet. May 22, 2013.

[16] Kramek, Joseph. *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities*. Brookings, July 2013.

[17] CVE-2016-5817, NIST, August 22, 2016.

[18] N4Rail Autostow. Navis.

[19] Maritime Jurisdiction. U.S. Department of Justice.

[20] Schmitt, Michael N., ed. *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press, 2017.

[21] Zukunft, Paul. *United States Coast Guard Cyber Strategy*. US Coast Guard. June 2015.

[22] MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems. International Maritime Organization. 2017.

[23] BIMCO et. al. *The Guidelines on Cybersecurity Onboard Ships*. Vol. 3 2018.