2016-06

Maritime cybersecurity: the future of national security

Hayes, Christopher R

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MARITIME CYBERSECURITY: THE FUTURE OF NATIONAL SECURITY

by

Christopher R. Hayes

June 2016

Thesis Advisor: Erik Dahl
Second Reader: Wade Huntley

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE MARITIME CYBERSECURITY: THE FUTURE OF NATIONAL SECURITY	**5. FUNDING NUMBERS**
6. AUTHOR Christopher R Hayes	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT

Cybersecurity in the 21st century is constantly evolving and changing in order to meet today's threats. The maritime industry in the United States is no different than any other organization that can fall under a cyber-attack. Currently, no major cyber threat has threatened the maritime community in the United States or national security. Recent attempts to disrupt the flow of the maritime industry, however, legitimize fears over maritime cyber-attacks.

The United States has significant shortfalls in maritime cybersecurity. This thesis evaluates U.S. ports and strategies against those of the European Union to examine the impact of cyber issues on the United States and its national security. The maritime community is not cyber resilient and has no specific guidelines or responses in place to deter or prevent a major cyber-attack on the United States. For the United States to maintain its cyber resilience and normal operations at its ports, the global maritime community must address the issues together to maintain global maritime dominance.

14. SUBJECT TERMS maritime, maritime cybersecurity, national security, ports, terminals, coast guard	**15. NUMBER OF PAGES** 97
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

MARITIME CYBERSECURITY: THE FUTURE OF NATIONAL SECURITY

Christopher R. Hayes
Lieutenant, United States Navy
B.A., State University of New York Maritime College, 2010

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
June 2016**

Approved by: Erik Dahl
Thesis Advisor

Wade Huntley
Second Reader

Mohammed M. Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Cybersecurity in the 21st century is constantly evolving and changing in order to meet today's threats. The maritime industry in the United States is no different than any other organization that can fall under a cyber-attack. Currently, no major cyber threat has threatened the maritime community in the United States or national security. Recent attempts to disrupt the flow of the maritime industry, however, legitimize fears over maritime cyber-attacks.

The United States has significant shortfalls in maritime cybersecurity. This thesis evaluates U.S. ports and strategies against those of the European Union to examine the impact of cyber issues on the United States and its national security. The maritime community is not cyber resilient and has no specific guidelines or responses in place to deter or prevent a major cyber-attack on the United States. For the United States to maintain its cyber resilience and normal operations at its ports, the global maritime community must address the issues together to maintain global maritime dominance.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAPA	American Association of Port Authorities
AIS	automatic identification system
APT	advanced persistent threat
CERT-EU	computer emergency response teams
CIIP	critical infrastructure protection plan
CG-FAC	Coast Guard Office of Port and Facility Compliance
CSCO	cybersecurity operations center
CSDP	Common Security and Defence Policy
CSITT	cyber strategy implementation team
DHS	Department of Homeland Security
ECDIS-N	Electronic Chart Display and Information System-Navy
EDA	European Defense Agency
ENISA	European Network and Information Security Agency
EO	executive order
EU	European Union
EUMSS	European Union Maritime Security Strategy
ERI	Ergon Refining, Incorporated
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GPS	global positioning system
HSCSD	Houston Ship Channel District
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IT	information technology
ICT	information and communications technology
ICS	industrial control system
IMO	International Maritime Organization
IRISL	Islamic Republic of Iran Shipping Lines
JCCC	joint command and control center
LMS	logistics management system
MARAD	maritime administration

MDA	maritime domain awareness
MPA	Maryland Port Authority
MMT	Magnolia Marine Transportation
MODU	mobile offshore drilling unit
MTS	Marine Transportation System
MTSA	Maritime Transportation and Security Act
NATO	North American Treaty Organization
NCIJTF	National Cyber Investigative Joint Task Force
NIS	network and information security
OCIA	Office of Cyber and Infrastructure Analysis
PAC	Ports America Chesapeake
PBM	Port of Beaumont
PHA	Port of Houston Authority
PLA	Port of Los Angeles
PLB	Port of Long Beach
POB	Port of Baltimore
POH	Port of Houston
POV	Port of Vicksburg
PPD	presidential policy directive
PSGP	Port Security Grant Program
RFID	radio frequency identification tag
RO-RO	roll-on/roll-off
SAFE	Security and Accountability for Every Port Act
SCADA	Supervisory Control and Data Acquisition
SOLAS	Safety of Life at Sea
SSA	sector-specific agency
TEU	twenty-foot equivalent unit
U.S.	United States
U.S.C.G	United States Coast Guard
USN	United States Navy
USNS	United States Navy Ship
USNI	United States Naval Institute

USTRANSCOM	United States Transportation Command
VPS	virtual port system
VLCC	very large crude carrier
VHF	very high frequency
WWII	World War II

THIS PAGE INTENTIONALLY LEFT BLANK

I. MARITIME CYBERSECURITY: THE NEW RULES OF THE ROAD

> America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas.
>
> —President Barack Obama[1]

A. MAJOR RESEARCH QUESTION

Cybersecurity is of grave importance to the maritime industry. As a recent article in the Naval Institute Proceedings noted, "maritime shipping moves 90-94 percent of world trade."[2] With a majority of the world's goods traveling through sea lanes, it is crucial for members of the maritime industry to understand the risks associated with the maritime cyber domain. This thesis evaluates the weaknesses of maritime cybersecurity through case studies and recent events to determine vulnerabilities in the maritime community. In particular, this thesis examines the following questions: to what extent do cyber vulnerabilities of non–U.S. flagged commercial vessels constitute a threat to U.S. national security, and what should be done to address those vulnerabilities?

B. IMPORTANCE

The maritime industry is reactive in setting standards and procedures based on catastrophic events. To cite a famous example, on April 15, 1912, the "unsinkable" RMS *Titanic* collided with an iceberg during her first underway from Southampton, United

---

[1] White House.gov, "Foreign Policy: Cybersecurity," accessed April 8, 2016, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity.

[2] Don Walsh, "Oceans - Maritime Cyber Security: Shoal Water Ahead?" *Proceedings Magazine* 14, no. 7 (2015): 1–2, http://www.U.S.Ni.org/magazines/proceedings/2015–07/oceans-maritime-cyber-security-shoal-water-ahead.

Kingdom, while traveling to New York City.[3] Believed by many to be indestructible, the *Titanic* departed on her maiden voyage with a minimum of lifeboats and lifejackets for the crew and passengers; the lack of safety equipment contributed to more than 1,500 deaths.[4] In response, the international community in 1913 came together for the Safety of Life at Sea (SOLAS) Convention to set international shipping practices and regulations for seafaring vessels.[5] Responding to the *Titanic* disaster, in 1914, maritime leaders worldwide mandated safety requirements, including durability, loading, capacity, and specific lifeboat building requirements, and required every person aboard have access to a lifejacket due to the negligence of the maritime community to spot these problems from the beginning.[6]

Today, the maritime industry has what will be referred to in this thesis as "*Titanic* syndrome." In the context of cyber threats, this means that the international community usually acts only in response to extraordinary events that place states in cyber panic. Maritime cyber-attacks are happening more frequently than members of the maritime community believe because of the number of unreported and undetected attacks.[7] Although research has suggested the maritime industry is vulnerable to cyber-attacks, very little has been done to prevent or deter them. During a presentation to the Naval Postgraduate School student body in March 2015, Vice Chief of Naval Operations Admiral Michelle Howard stressed the growing concerns the United States Navy (USN) has regarding maritime cybersecurity and its potential threats. Admiral Howard stresses the importance again during an interview with the *Navy Times*:

---

[3] History, "This Day in History: April 15," accessed February 4, 2016, http://www.history.com/this-day-in-history/titanic-sinks.

[4] Ibid.

[5] Dan Bender, "How the Sinking of the Titanic Changed the World," *Coast Guard Compass*, Official Blog of the U.S. Coast Guard, April 14, 2010, last Accessed February 4, 2016, http://coastguard.DoDlive.mil/2010/04/how-the-sinking-of-the-titanic-changed-the-world/.

[6] International Convention for the Safety of Life at Sea, 1974, accessed April 25, 2016, http://www.ifrc.org/docs/idrl/I456EN.pdf.

[7] "Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas," CyberKeel, October 15, 2105, http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf.

> My perspective is that everyone is the cyber, active, reserve, and civilians. We operate and live in this domain. There's not a person in the Department of the Navy who probably doesn't have a desktop, doesn't deal with Microsoft products, Excel spreadsheets, databases, transference of data, email, and so we are all in this domain.[8]

The concerns of the USN are valid as state actors, such as China and Russia, have been advancing their capabilities for cyber warfare.[9] These cyber-attacks, therefore, trickle down into the merchant sector, which has fewer capabilities and less resilience to defend against such attacks.

In order for the maritime industry to remain successful, the industry must be forward thinking to become more resilient through standardized plans and procedures. Despite outside research, however, very little has been done to address recent attacks, equipment vulnerabilities, or needed technological development. Though challenges in today's cyber domain have led to denial of services and, thus, to a disruption in the supply chain, the maritime industry still has no global standards in place for maritime cybersecurity.

Government agencies invest in maritime cybersecurity and the protection of critical U.S. infrastructure. However, the job of protecting America's maritime cyber-interests has become difficult because many of the ships in today's maritime fleet that enter the United States are non–U.S. flagged vessels and crewed by foreigners.[10] In 2004, the U.S. Department of Transportation's Maritime Administration Office of Financial and Rate Approvals drew attention to "the nationalities and size of the crews of foreign-flag

---

[8] Sam Fellman, "VCNO Michelle Howard pushes for cyber vigilance, more women in the ranks," *Navy Times*. April 12, 2015, http://www.navytimes.com/story/military/pentagon/2015/04/12/vcno-michelle-howard-cyber-vigilance-more-women-navy-ranks/70774264/.

[9] Arshad Mohammed, Matt Spetalnick, and Mark Hosenball, "Exclusive: U.S. Weighs Sanction Russia as well as China in Cyber Attacks," *Reuters*, September 1, 2015, http://www.reuters.com/article/2015/09/01/us-usa-cybersecurity-russia-exclusive-idUSKCN0R12FE20150901#0wKGvOQlmoE6SXDF.97.

[10] "Foreign-Flag Crewing Practices: A Review of Crewing Practices in U.S.–Foreign Ocean Cargo Shipping," U.S. Department of Transportation Maritime Administration, November 2006, 3, http://www.marad.dot.gov/wpcontent/uploads/pdf/Crewing_Report_Internet_Version_in_Word-update-Jan_final.pdf.

cargo vessels calling at ports in the United States."[11] The number of foreign mariners entering out ports daily raises red flags for cyber awareness and training. Released in 2006, the report analyzes the top five port concentration areas in the United States: Houston, Los Angeles/Long Beach, Miami, Newark/New York, and New Orleans.[12] The top five flags for ships entering these ports are in numerical order, starting with the most prevalent: Panama, Liberia, Cyprus, Malta, and the Bahamas. The top five nationalities of crewmembers on the commercial ships entering the ports are in numerical order starting with the most prevalent: Philippines (36.6%), China (9.3%), India (8.1%), Ukraine (5.4%), and Russia (4.9%).[13] The report concludes, "crewmembers from 123 different countries were found on foreign-flagged vessels calling U.S. ports."[14] With so many different stakeholders and nations involved, regulating the vessels entering U.S. ports under a U.S. cybersecurity standard will be difficult to enforce. For the United States to be successful in implementing procedures to protect its interests, the international community must put forth cybersecurity deliverables that are both agreeable and beneficial to the global maritime community.

C. PROBLEMS AND HYPOTHESIS

This thesis evaluates different parts of the maritime community through historical contexts, including legislation, governance, and recent reviews, to demonstrate the seriousness of maritime cyber threats for national security. The maritime domain is a vast network of different institutions and players that must work in unison to prevent and deter maritime cyber-attacks. Many researchers have found that there are significant cybersecurity weaknesses within the maritime community, which the community itself does not take seriously enough.

---

11 "Foreign-Flag Crewing Practices," U.S. Department of Transportation Maritime Administration, 3.

12 Ibid, 6.

13 Ibid, 9–10.

14 Ibid, 10.

The primary hypothesis of this thesis is that the maritime community in the United States takes maritime cybersecurity for granted, leading to serious gaps in U.S. national security. Despite countless written articles, the maritime community has taken a limited approach toward defending the cyber realm.

The secondary hypothesis of this thesis is that if we are to have a resilient maritime domain, the United States must ratify worldwide maritime cyber-domain standards and convince world leadership to ratify such standards in protecting maritime interests. The security of the global commercial fleet and port infrastructure relies on the international community to adopt legislation that regulates technology both afloat and ashore. Industry success means the international community must work more vigorously to enforce a minimum level of cybersecurity. Global cybersecurity requirements led by the International Maritime Organization (IMO) relieve the burden placed on entities in the United States. In return, the United States can focus its efforts on maintaining international laws. The potential issue with this hypothesis is that it requires the international community to fund and regulate programs that all maritime countries agree upon for international maritime cybersecurity.

D. LITERATURE REVIEW

The purpose of this literature review is to establish a baseline for understanding maritime cybersecurity policies and literature specific to the major research question. Not only do experts in cybersecurity fear that U.S. ports are suffering from negligent cybersecurity but also that ships entering the United States are at risk because of advancements in technology.[15] Experts from the Heritage Foundation, the United States Naval Institute (USNI), the United States Coast Guard (USCG), CyberKeel, the European Network and Information Security Agency (ENISA), the Department of Homeland Security (DHS), and other maritime-concerned parties of the private and public sectors agree that action must be taken to prevent the potential crisis of a severe maritime cyber-

[15] Thad Odderstol, "C-Cubed: Increasing Cyber Resilience, Awareness, and Managing Risk," *Coast Guard Proceedings* 71, no. 4 (2014–2015): 12, http://uscgproceedings.epubxp.com/i/436751-win-2015.

attack. In order to determine whether U.S. national security assets are at risk, it is crucial to define maritime cybersecurity and identify responsibility for maritime cybersecurity in the United States in terms of national security.

1. Defining Maritime Cybersecurity, Attacks, and Domain

The maritime community has yet to establish a global definition for "maritime cybersecurity." This thesis accepts Merriam-Webster's definition of *cybersecurity*: "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack."[16] This thesis defines *maritime cybersecurity* as measures taken to protect network and computer assets both on ships, terminals, ports, and all computerized equipment supporting maritime operations. A *cyber-attack* is any "attempt to damage, disrupt, or gain unauthorized access to a computer system, or electronic communications network."[17] Cyber-attacks pertain to the same computer assets on ships, terminals, ports, and all computerized equipment supporting maritime operations. The *Maritime domain* is defined as "all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances."[18] *Resilience* is defined as "an ability to recover from or adjust easily to misfortune or change."[19] For the purposes of this thesis, *maritime cyber resilience* means the ability of the maritime community to recover after a cyber-attack.

---

16 *Merriam-Webster Dictionary*, s.v. "Cybersecurity," accessed April 8, 2016, http://www.merriam-webster.com/dictionary/cybersecurity.

17 *Dictionary.com*, s.v. "Cyber-attack," accessed April 8, 2016, http://www.dictionary.com/browse/cyber-attack. No official international or U.S. definition is available as of May 2016.

18 "National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security," Department of Homeland Security, October 2005, i, https://www.dhs.gov/sites/default/files/publications/HSPD_MDAPlan_0.pdf.

19 *Merriam-Webster Dictionary*, s.v. "Resilience," accessed May 2, 2016, http://www.merriam-webster.com/dictionary/resilience.

2. United States Maritime Cybersecurity Governance

The world's reliance on technology is expanding every day, and the ability to infiltrate computer-based networks is expanding. The events of September 11, 2001 will forever change the way the United States handles security operations. Congress passed the Maritime Transportation and Security Act (MTSA) in 2002 and the Security and Accountability for Every (SAFE) Port Act in 2006. Both of these acts mandated specific requirements for physical security at ports including patrol boats, waterside security, and entrance control points. Although legislation was put in place to secure ports in the United States, the cyber realm has remained practically untouched.[20]

President Obama signed two different policies to ensure critical infrastructure in the United States is protected against the evolving cyber threat: Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience* and Executive Order (EO) 13,636, *Improving Critical Infrastructure Cybersecurity*.[21] According to Danielle Bivens, PPD 21 "guides efforts to secure, strengthen, and maintain the nation's critical infrastructure and directs critical infrastructure owners and operators to work together and share responsibility."[22] The overarching principle of PPD 21 is the ability to allocate federal, state, and private entities working in unison in defense of maritime infrastructure. The ability of information-sharing among key members in the maritime industry makes the response and recovery time more sustainable for all parties involved and allows port operations to return to normal. PPD 21 also defines a *sector-specific agency* (SSA) as an agency responsible for critical infrastructure. PPD 21 establishes responsibly of cyber threats domestically:

> The FBI also conducts domestic collection, analysis, and dissemination of cyber threat information, and shall be responsible for the operation of the National Cyber Investigative Joint Task Force (NCIJTF). The NCIJTF

---

[20] "10 Years after 9/11, Security Still a Top Priority of U.S. Ports," Maritime Executive, September 2, 2011, http://www.maritime-executive.com/article/10-years-after-9–11-security-still-a-top-priority-of-u-s-ports.

[21] Danielle Bivens, "Maritime Governance: Designed with security in mind," *Coast Guard Proceedings* 71, no. 4 (2014–2015): 6, http://uscgproceedings.epubxp.com/i/436751-win-2015.

[22] Ibid.

> serves as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from DHS, the Intelligence Community (IC), the Department of Defense (DOD), and other agencies as appropriate.
>
> The Department of Commerce (DOC), in collaboration with DHS and other relevant Federal departments and agencies, shall engage private sector, research, academic, and government organizations to improve security for technology and tools related to cyber-based systems, and promote the development of other efforts related to critical infrastructure to enable the timely availability of industrial products, materials, and services to meet homeland security requirements.[23]

PPD 21 establishes the basic framework for overall security, both physical and cyber, for the United States' critical infrastructure. EO 13636 specifically focuses on cybersecurity as it pertains to critical infrastructure:

> Executive Order 13636 … calls for various actions to improve the cybersecurity of critical infrastructure. These include developing a cybersecurity framework; increasing the volume, timeliness, and quality of cyber threat information shared with the U.S. private sector; considering prioritized actions within each sector to promote cybersecurity; and identifying critical infrastructure for which a cyber incident could have a catastrophic impact.[24]

Prior to PPD 21 and Executive Order 12636, President George W. Bush signed Presidential Directive 12, *Maritime Security Policy*, which outlined policy objectives and guidelines for U.S. maritime interests.[25] The policy set by President Bush gave way to the National Plan to Achieve Maritime Domain Awareness (MDA). The purpose of the MDA plan, as outlined by Danielle Bevins, is for key management and security managers

---

[23] Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, February 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[24] Gregory C. Wilhusen, "Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity," United States Government Accountability Office, October 8, 2015, 2, http://gao.gov/assets/680/672973.pdf.

[25] National Security Presidential Directive (NSPD) 41/Homeland Security Presidential Directive (HSPD) 13, December 21, 2004, 1, https://fas.org/irp/offdocs/nspd/nspd41.pdf.

in various parts of the maritime community to increase their awareness of potential cyber-attacks on ports in the United States through the following measures:

> Enhancing maritime domain transparency to detect, deter, and disrupt threats, as early as possible;
>
> Enabling accurate, dynamic, and confident decisions and responses to the full spectrum of maritime threats and challenges through information sharing;
>
> Facilitating partnerships to promote maritime domain information sharing, safeguarding, capacity building, and integration;
>
> Preserving our [U.S.] rights, freedoms of navigation and overflight, and uses of the sea and airspace recognized under international law, while promoting lawful, continuous, and efficient commerce flow.[26]

Although these requirements were established in 2005, many members of the maritime community do not meet the requirements out of ignorance or failure to prioritize cybersecurity as a major national threat.

E. SUMMARY AND THESIS OVERVIEW

Today, the maritime community as a whole is insecure due to its own ignorance about maritime cybersecurity. Potential actors can harm the U.S. maritime community without notice and with the ability to escape unpunished. This thesis argues that the question is not when will a maritime cyber-attack take place, but how bad will the attack be? Even more broadly, the United States is not ready to recover or respond from a serious cyber-attack at its ports. Although legislation has passed on maritime cybersecurity, little has been done about enforcing a unified standard of protection. This thesis examines these threats and recommends that the maritime community rethink its posture toward cybersecurity in the 21st century.

This thesis uses a comparative approach in examining cybersecurity in the maritime domain of the United States. It consists of five chapters.

---

[26] Bivens, "Maritime Governance," 7.

Chapter II presents recent attacks and incidents affecting the maritime industry, a review of the actors behind a maritime cyber-attack, and the seriousness of a cyber-attack for U.S. national defense.

Chapter III evaluates six different ports in the United States that were initially examined in a Brookings study and illustrates the vulnerabilities in our maritime cyber infrastructure.

Chapter IV evaluates the roles of the federal, state, and local actors who are responsible for the overall resilience of cybersecurity at U.S. ports.

Chapter V concludes by examining the threat of a maritime cyber-attack on the United States, providing policy recommendations, and suggesting areas for further research.

II. MARITIME CYBERSECURITY: RECENT ATTACKS AND INCIDENTS

> I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.
>
> —former Director FBI Robert S. Mueller III[27]

Why do individuals or states conduct maritime cyber-attacks? According to Lars Jensen, an expert in maritime cybersecurity, an attacker's motivation ranges from financially to smuggling in contraband to stealing company secrets from different marine industries. [28] Afloat and ashore, the maritime industry operates sensitive equipment that is easily accessible through the Internet. Many users of navigational or logistic software, for example, have necessary skills and schooling to operate the equipment, but when faced with technical issues, these same operators usually need information-technology (IT) support.[29] Lacking certain IT skillsets leaves operators defenseless and companies vulnerable to losing information, equipment, or profit.

CyberKeel, a maritime cyber-security firm located in Denmark, argues that maritime cyber defense should not be taken lightly. CyberKeel believes that every operator aboard a ship or terminal[30] needs to be aware of the potential threats from cyber-attacks to recognize an arising issue.[31] A white paper published by CyberKeel outlines the thoughts of top-tier decision makers regarding maritime cybersecurity:

---

[27] Robert S. Mueller III, "Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies," Speech for the RSA Cybersecurity Conference, San Francisco, CA, March 1, 2012, https://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[28] Lars Jensen, "Challenges in Maritime Cyber-Resilience," *Technology Innovation Management Review* 5, no 4. (April 2015): 37, http://timreview.ca/article/889.

[29] "Maritime Cyber-Risks," CyberKeel.

[30] A terminal is any part of a port or shipping facility that handles shipping containers or cargo.

[31] "Maritime Cyber-Risks," CyberKeel, 3.

> Cybersecurity is a technical matter largely delegated to the IT manager, or the CIO, and is not something materially involving the CEO, CCO, COO, CFO or the HR Manager. A belief that the cyber threats are chiefly theoretical in nature, usually linked to a doubt as to whether there is anyone with a genuine motivation to perform cyberattacks against their own particular maritime company.[32]

This chapter demonstrates how serious the cyber threat is toward the maritime industry. First, it reviews several of the most significant, recent maritime cyber-attacks. Second, this chapter reviews maritime technologies and how they pose a risk. Third, it examines the players who are responsible for the cyber threat. Finally, this chapter synthesizes evidence from port closures in the United States and testimonies to Congress to demonstrate the repercussion of the cyber threat in today's maritime domain.

A. RECENT MARITIME CYBER-ATTACKS

Cyber-attacks on the industry are taking place; whether companies want to acknowledge these attacks is a different story. Cyber threats and vulnerabilities may include exploiting banking records, accessing logistical software, as well as taking control of ships' navigation and engine controls. This section examines four documented attacks: the cyber-attack on the Islamic Republic of Iran Shipping Lines, the Icefog virus, the first case of ghost shipping, and inadvertent network breaches on mobile offshore drilling units (MODUs).

1. The Islamic Republic of Iran

With multilateral sanctions placed on Iranian exports by the international community, shipping plays an important part in keeping Iran's economy alive. In August 2011, the Islamic Republic of Iran Shipping Lines (IRISL), an Iranian state-owned shipping company, fell victim to a cyber-attack.[33] Lars Jenson, founder of CyberKeel, reported, "The attacks damaged all the data related to rates, loading, cargo number, date

---

[32] "Maritime Cyber-Risks," CyberKeel, 4.

[33] Yeganeh Torbati and Jonathan Saul, "Iran's Top Cargo Shipping Line Says Sanctions Damage Mounting," *Reuters*, October 22, 2012, http://www.reuters.com/article/us-iran-sanctions-shipping-idUSBRE89L10X20121022.

and place … resulting in severe financial losses."[34] According to Mohammad Hussein Dajmar, Managing Director of IRISL, the cyber-attacks took cargo and general shipping information from the line, and because of the severity of the attack, Dajmar believes outside governments were involved.[35] The amount of data lost from this cyber-attack made it almost impossible for Iranian stevedores to account for containers placed on ships or stored pier-side without having to individually verify all twenty-foot equivalent units (TEU). Although Dajmar did not say how long it took to restore his company to normal operations, he did admit "there was considerable damage."[36]

A separate cyber-attack took place in Iran in October 2012. Officials from Tehran reported that cyber-attacks had targeted communication networks established on offshore oil and gas platforms in the Persian Gulf.[37] With Iranian exported oil peaking at 79 percent of its gross domestic product in 2014, the Iranian government and its investors have worried that any shut-down to oil networks will have catastrophic repercussions on the Iranian economy.[38] Cyber-attacks and threats on Iranian critical infrastructure have pushed Tehran to invest heavily in cyber defense and capabilities.[39] Since 2012, Tehran has not made public any other cyber-attacks against its maritime components.

2. "Icefog"

In 2013, Internet security conglomerate Kaspersky Labs released evidence of ongoing phishing attacks since early 2001 on Japanese and South Korean assets. According to the company, targets of the phishing included "governmental institutions, military contractors, maritime and shipbuilding groups, telecom operators, industrial and

---

[34] "Maritime Cyber-Risks," CyberKeel, 6.

[35] Ibid.

[36] Torbati and Saul, "Iran's Top Cargo Shipping Line."

[37] "Iran's Offshore Platforms Become Target," Maritime Executive.

[38] Daniel Workman, "Iran's Top 10 Exports," *World's Top Exports*, August 29, 2015, http://www.worldstopexports.com/irans-top-10-exports/; MarEx. "Iran's Offshore Platforms Become Target to Recent Cyber Attacks." The Maritime Executive. October 9, 2012. http://maritime-executive.com/article/iran-s-offshore-platforms-become-target-of-recent-cyber-attacks.

[39] Bill Gert, "Iran Rapidly Building Cyber Warfare Capabilities," *The Washington Free Beacon*, May 12, 2015, http://freebeacon.com/national-security/iran-rapidly-building-cyber-warfare-capabilities/.

high-tech companies and mass media."[40] This type of attack is known by cyber experts as an advanced persistent threat (APT), "a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network."[41]

To gain access to the Japanese and South Korean networks, according to Kaspersky, the attackers masked a backdoor entry known as Fucobha:

> The "Icefog" backdoor set (also known as "Fucobha") is an interactive espionage tool that is directly controlled by the attackers. There are versions for both Microsoft Windows and Mac OS X. In its latest incarnation, Icefog doesn't automatically [infiltrate] data[;] instead, it is operated by the attackers to perform actions directly on the victim's live systems. During Icefog attacks, several other malicious tools and backdoors were uploaded to the victims' machines, for data exfiltration and lateral movement.[42]

Once inside the system, the hackers stayed undetected while extracting whatever data the group was after.[43] Effective backdoor entry to servers guaranteed a high success rate for Icefog. Kaspersky traced the origin of Icefog back to exploitations in Java programs and within the Microsoft Office and Mac OS X operating systems.[44] At the time of the study, Kaspersky Labs exposed six different backdoor variants of Icefog:

> The "old" 2011 Icefog—which sends stolen data by e-mail; this version was used against the Japanese House of Representatives and the House of Councilors in 2011.
>
> Type "1" "normal" Icefog—which interacts with command-and-control servers.

---

40 "The 'Icefog' Apt: A Tale of Cloak and Three Daggers." Kaspersky Lab, 2013, http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/icefog.pdf.

41 *Tech Target*, s.v. "Advanced persistent threat (APT)," accessed April 2, 2016, http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.

42 "The 'Icefog' Apt," Kaspersky.

43 "Maritime Cyber-Risks," CyberKeel, 7.

44 Kaspersky Lab, "Kaspersky Lab exposes 'Icefog': a new cyber-espionage campaign focusing on supply chain attacks," September 26, 2013, http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_exposes_Icefog_a_new_cyber-espionage_campaign_focusing_on_supply_chain_attacks.

> Type "2" Icefog—which interacts with a script-based proxy server that redirects commands from the attackers to another machine.
>
> Type "3" Icefog—We (Kaspersky) don't have a sample of this variant but we observed a certain kind of C&C (command and control) that uses a different communication method; we suspect there are victims infected with this malware.
>
> Type "4" Icefog—same situation as "type 3."
>
> Icefog-NG—which communicates by direct TCP (Transmission Control Protocol) connection to port 5600.[45]

Once Kaspersky Labs composed and publically released its report on Icefog, the threat and hackers soon disappeared from the Internet. The findings enabled IT security companies around the world to verify system networks to see whether Icefog had also affected their grids. With the availability of IP addresses for Icefog, one unnamed U.S. oil and gas company concluded its systems had been compromised without knowing the exact information taken or how long its systems had been penetrated.[46]

3. Ghost Shipping

Drug traffickers are cashing in on the vulnerabilities surrounding shipping network systems. Between 2011 and 2013, Dutch drug traffickers employed computer savvy counterparts to hide cocaine inside containers enroute to the Port of Antwerp by infiltrating networks responsible for managing what was inside each TEU.[47] According to CyberKeel, the hackers were able "to have remote access to the terminal systems, and thereby they [drug traffickers] were able to release containers to their own truckers without knowledge of the port or the shipping line."[48] Employees noticed that containers were continually disappearing from the port and reported the attacks to local authorities.

---

45 "The 'Icefog' Apt," Kaspersky.

46 Mike Lennon, "'Icefog' Cyber Attacks Targeted U.S. Energy Firms Using Java Backdoor," *Security Week*, January 14, 2014, http://www.securityweek.com/icefog-cyber-attacks-targeted-us-energy-firms-using-java-backdoor.

47 Tom Bateman, "Police Warning after Drug Traffickers' Cyber-attack," *BBC News*, October 16, 2013, http://www.bbc.com/news/world-europe-24539417.

48 "Maritime Cyber-Risks," CyberKeel, 8.

According to Dutch prosecutors, smugglers had placed drugs in containers of commercial goods departing from South America to Antwerp in hopes of going unnoticed. When the shipments arrived, traffickers arrived in trucks and produced false bills of lading to take custody of the containers with commercial goods and drugs. By the time the rightful owners of the TEUs arrived with proper bills of lading, the traffickers had already taken delivery of the shipments. The stevedores believed they had turned the TEUs to the rightful owners because the networks reflected this information. Eventually, security officers informed higher authorities, and police raided the suspects' hideout, finding hacking devices, drugs, 1.3 million Euros, and firearms.[49]

Danny Decraene, the head of Antwerp's organized crime unit states, “These criminal organizations always look for a new way to get drugs out of the harbor. In this case, they hired hackers [who were] very high level, intelligent guys, doing a lot of software work.”[50] Director of Europol Rob Wainwright believes this is a “new business model” for drug traffickers who are looking to expose the cyber community, especially in the maritime sector. Wainwright believes in order to stay ahead in the cyber domain, local authorities must learn to become more tech-savvy and governments must provide thorough legislation to support the police authorities.[51] To this day, the amount of drugs smuggled in and out of the port is still unknown.

Penetrating networks in this fashion has been coined “ghost shipping,” and the Antwerp case was the first known breach of its kind.[52] Australian customs discovered a similar attack in 2012. Criminals hacked logistic software to determine whether Australian customs tracked its containers. If cargoes went unnoticed by custom officials, the group would intercept the shipments. If the group sensed its containers were at risk, it simply abandoned the cargo at the pier to avoid being caught.[53]

---

[49] Bateman, “Police Warning.”

[50] Ibid.

[51] Bateman, “Police Warning.”

[52] “Maritime Cyber-Risks,” CyberKeel, 8.

[53] Ibid.

4. Mobile Offshore Drilling Units

Mobile offshore drilling units (MODUs) enable gas and oil companies to drill for untapped resources offshore. In 2013, while drilling in the Gulf of Mexico, workers from a U.S.-based oil company accidently uploaded malware onto the main computing system of the MODU. The effects of this attack paralyzed the rig, particularly from communicating with the rig's navigation system. A worker had unintentionally introduced malware through a thumb drive, which held previously corrupted pornographic images and illegal music.[54] According to the after action report, the corrupted files that had been downloaded from the Internet "crossed over to the rig's computer systems when the devices were plugged in."[55] Thrusters and navigational equipment aboard the MODU were immobilized, causing the MODU to drift away from the drilling site, consequentially cutting into production time.[56]

Two similar cases involving offshore drilling equipment have been made public. The first breach caused an oil rig to unbalance itself, resulting in the loss of seven days of production. The second case involved the transportation of a rig from South Korea to Brazil, during which malware penetrated the propulsion system and delayed delivery by 19 days.[57] Although these attacks caused monetary losses, researchers believe future breaches on MODUs will cause environmental damage through oil spills and loss of life through explosions.[58]

5. Summary

The maritime community is quite reactive instead of proactive toward cyber threats. Criminals with the ability to pass illicit drugs through a port simply by accessing

---

[54] Sonja Swanbeck, "Coast Guard Commandant Addresses Cybersecurity Vulnerabilities on Offshore Oil Rigs," *CSIS Strategic Technologies Program*, June 22, 2015, http://www.csistech.org/blog/2015/6/22/coastguard-commandant-addresses-cybersecurity-vulnerabilities-in-offshore-oil-rigs.

[55] Ibid.

[56] Ibid.

[57] Ibid.

[58] Kate B. Belmont, "Maritime Cyber Attacks: Changing Tides," Blank Rome Counselors at Law, November 16, 2015, https://www.blankrome.com/index.cfm?contentID=37&itemID=3734.

logistical software and creating false bills of lading, such as in the ghost shipping case, should pique concern for responsible parties in U.S. national security. Some penetrations are inadvertent, as the MODU example illustrated. Government officials and the maritime industry must learn from the recent cyber-attacks to keep U.S. ports and interests open.

B. EQUIPMENT VULNERABILITIES IN SHIP SYSTEMS

Today's mariners rely heavily on networks, systems, and outside sources for navigation. Many significant cyber threats are the result of vulnerabilities in equipment carried and used by the maritime industry worldwide. Equipment vulnerable to cyber-attacks includes navigation systems, and this section reviews four of those critical systems: the automatic identification system (AIS), global positioning system (GPS), industrial control system (ICS), and Electronic Chart Display Information System (ECDIS).

1. Ships Disappearing from the Automatic Identification System

AIS is a shipboard safety feature placed on all commercial or military ships over 1,600 gross tons that allows mariners to obtain valuable information about other vessels.[59] 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. The complexity and resources employed for AIS is referenced in Figure 1.[60]

---

[59] Lee Ferran, "The Guys Who Can Make Oil Tankers Disappear, Virtually," *ABC News*, Oct 15, 2013, http://abcnews.go.com/Blotter/guys-make-oil-tankers-disappear-virtually/story?id=20565851.

[60] Allison Middleton, "Hide and Seek: Managing Automatic Identification System vulnerabilities," *Coast Guard Proceedings* 71, no. 4 (2014–2015): 49, http://uscgproceedings.epubxp.com/i/436751-win-2015.

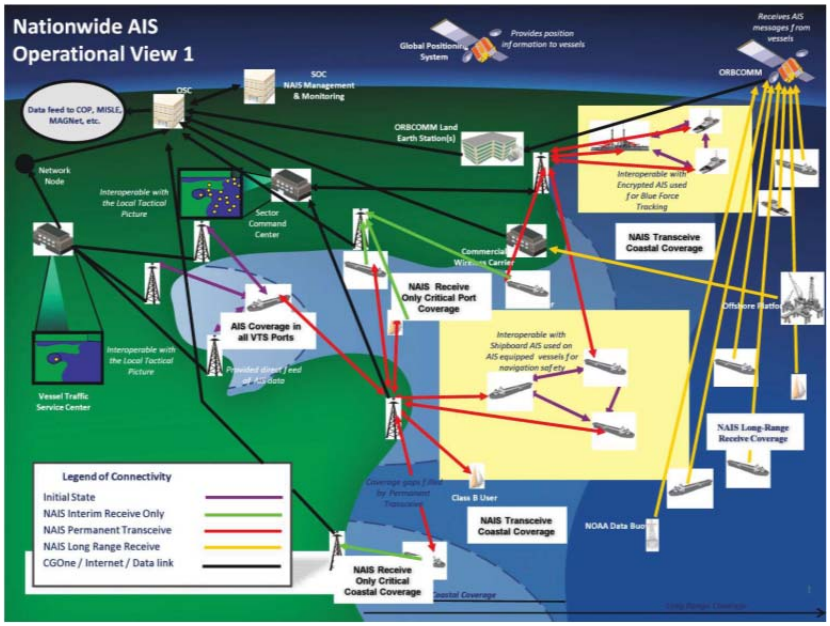

Figure 1. AIS Overview from Coast Guard Proceedings[61]

Vulnerabilities in the AIS system are widely known. For example, a study conducted by the Trend Micro Forward-looking Threat Team, a threat defense group that focuses on the technology sector, was able to recreate a VHF frequency on AIS that simulated a "ghost ship" in a harbor and alerted nearby vessels they were on a collision course with another vessel.[62] Furthermore, Trend Micro exposed a full list of AIS "spoofing" abilities including false course, speed, ship flag and name; false weather alerts causing digresses from original plan of intended movement; falsification as a maritime law enforcement authority (USCG); false maritime rescue platforms, false man overboard situations; and overwhelming of AIS leading to double reporting and false data causing system overloads.[63]

In 2012, Reuters exposed the illegal transportation of Iranian crude oil from Iran to China, India, and South Korea. Research exposed there were at least three Iranian ships flying a Tanzanian flag while pretending to be Syrian-owned in an attempt to avoid

---

[61] Source: Middleton, "Hide and Seek," 49.

[62] Ferran, "The Guys Who Can Make Oil Tankers Disappear."

[63] "Maritime Cyber-Risks," CyberKeel, 9.

a boarding and inspection of the containers.[64] Getting around international sanctions was easy for the Iranian oil company, which falsified its AIS data to reflect that of a Tanzanian ship. When questioned, officials representing the flagging agency in Tanzania denied these Iranian vessels as part of their registry.[65] The amount of illegal oil or other goods transported by these ships is unknown and exposes another weakness in technology on which the maritime industry relies.

A similar event took place in 2010 when a private fishing ship, illegally engaged in fishing activity in Argentinian waters, evaded the Argentinian Coast Guard by traveling outside the country's maritime borders and disabling AIS aboard the vessel. Although the Argentinian Coast Guard assumed the vessel had traveled outside its territorial waters, the coast guard was unable to track the vessel.[66] These cases suggest that as long as AIS is non-encrypted, problems will continue to remain, and legitimacy of data passed through the system will remain questionable.[67]

2. GPS Terrorism

In the early days of sailing, mariners were not worried about the sun, moon, or stars falling from the sky and, thus, losing the ability to navigate. Today, with the maritime world's heavy reliance on technology, GPS data is crucial to maintain safety of navigation at sea for all vessels.[68] Spoofing and jamming are two different techniques that wreak havoc on the maritime community whenever successfully employed. GPS spoofing is defined as "an electronic attack involving signals being sent to a receiver to

---

64 Jessica Donati and Daniel Fineren, "Exclusive: Iran Shipping Signals Conceal Syria Ship Movements," *Reuters*, December 6, 2012, http://www.reuters.com/article/us-syria-iran-tracking-idUSBRE8B50KX20121206.

65 Ibid.

66 Middleton, "Hide and Seek," 49.

67 "Maritime Cyber-Risks," CyberKeel, 9.

68 Brittany M. Thompson, "GPS Spoofing and Jamming: A Global Concern for All Vessels." *Coast Guard Proceedings* 71, no. 4 (2014–2015): 50, http://uscgproceedings.epubxp.com/i/436751-win-2015.

control navigation" whereas GPS jamming involves an actor intentionally blocking GPS signals.[69]

The Office of Cyber and Infrastructure Analysis (OCIA), a subgroup of DHS, has identified concerns for GPS jamming and spoofing for commercial shipping, primarily over mariners' overreliance on GPS systems and abandonment of traditional visual aids in navigating narrow channels. Operating near shoal water or in a narrow channel naturally increases the risk of navigational disasters such as grounding or collision. A loss of a ship's navigational inputs, steering, or propulsion would be catastrophic and cause significant damage, delays in services, and financial strains.[70] Another GPS incident took place in 2013 when four cranes were taken out of commission at a port in the United States for seven hours due to a GPS anomaly. Although this was not an attack, the anomaly reinforced the view that ships over-rely on GPS for maintaining port operations and the flow of goods and services.[71]

3. Industrial Control Systems

An industrial control system (ICS) is made up of multiple control systems aboard ships that feed into a central network. Smaller nodes aboard the vessel allow mariners to access different data regarding the ship's propulsion, navigation, and steering, to name a few. The diagram below is an example of the complexity of the systems[72]:

In July 2013, a group from the University of Texas accessed the ICS of a 210-foot yacht while the vessel was underway in the Mediterranean. With prior permission from the captain, the group had taken full control of the ship's navigation system and drove the yacht any way the group wanted.[73] The penetration exposed serious vulnerabilities to the

---

69 Thompson, "GPS Spoofing and Jamming," 50.

70 "Consequences to Seaport Operations from Malicious Cyber Activity," Office of Cyber and Infrastructure Analysis (OCIA), March 3, 2016, 11, http://www.maritimedelriv.com/Port_Security/DHS/DHS_Files/OCIA_Consequences_to_Seaport_Operations_from_Malicious_Cyber_Activity.pdf.

71 Ibid, 10.

72 "Consequences to Seaport Operations," OCIA, 4.

73 Thompson, "GPS Spoofing and Jamming," 50.

yacht's automatic navigation system and rudder control.[74] Captain Andrew Scholfield, Captain of the vessel, stated that his "team did a number of attacks and basically we on the bridge were absolutely unaware of any difference."[75] The ability for the team at the University of Texas to control a vessel over 6,000 miles away provides evidence that maritime systems as platforms are vulnerable no matter where they are in the world. Although the test was planned and controlled, it still surprised the captain that the transition to the red team was unnoticeable; the test raises questions about whom else might have the ability to penetrate a ship using this technique.

4. Electronic Chart Display and Information System Hacks

Paper charts are becoming a relic of the past. The Electronic Chart Display and Information System (ECDIS), a computer-based navigational chart display, has replaced paper charts. The many sensors around a typical commercial ship feed the following input into ECDIS: AIS, GPS data, speed, course, and radar.[76] As the primary means of navigation, the ECDIS system provides electronic digital charts that allow a mate of the watch on a civilian ship, or an officer of the deck (OOD) on a USN vessel to properly navigate. Receiving the most up-to-date chart information requires ECDIS systems to establish a connection through non-secure Internet networks aboard vessels, which could put the integrity of a ship's navigational data at risk.[77] In January of 2014, NCC Groups, an information assurance firm, played the role of a hacker trying to gain access to a ship's ICS. According to CyberKeel, after undergoing tests, "several security weaknesses were found including the ability to read, download, replace or delete any file stored on the machine hosting ECDIS."[78]

---

74 John Roberts, "Exclusive: GPS Flaw Could Let Terrorists Hijack Ships, Planes." *Fox News*. July 26, 2013. http://www.foxnews.com/tech/2013/07/26/exclusive-gps-flaw-could-let-terrorists-hijack-ships-planes.html; "Maritime Cyber-Risks," 11.

75 Ibid.

76 "Maritime Cyber-Risks," CyberKeel, 12.

77 Operational Analysis Division. "Consequences to Seaport Operations," 11.

78 "Maritime Cyber-Risks," CyberKeel, 12.

Overreliance on ECDIS data can be costly. On January 17, 2013, a U.S. Navy minesweeper, the USS *Guardian* (MCM 5), ran aground on the Tubbatatha Reef off the coast of the Philippines. Despite numerous alarms and warnings from the Navy's version of ECDIS (ECDIS-N), the navigation and bridge team disregarded visual cues and fixes as required under navy direction. Upon an investigation, the navy determined the minesweeper loaded the wrong charts prior to sea detail, thus landing the vessel aground. This event, although not a cyber-attack, depicts the navy ship's overreliance on electronic data.[79]

5. Summary

Technology is a mariner's best friend or worst enemy. Overreliance on these systems can create a false sense of security, especially while navigating or operating equipment on the high seas. The industry will be adversely affected in the near future with a growing cyber threat.

C. UNDERSTANDING THE PLAYERS

Different players and groups may have reasons to hack into terminal software to gain access to data, terminals, or a ship itself. The end goal for an individual or group will be different depending on what the overall goal is at the end of a mission. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) places cyber crooks into one of five categories: national governments, terrorists, industrial spies and organized crime groups, hacktivists, and hackers.[80] Any of these individuals or groups could cause more harm than another based on available resources and the type of cyber-attack planned.

National governments are the biggest threat to cyber-attacks due to the vast amount of resources and funding one government may have to employ against another According to the ICS-CERT, the goal of a government-sponsored cyber-attack on another

---

79 Operational Analysis Division. "Consequences to Seaport Operations," 11.

80 Marshall E. Newberry, "Maritime Critical Infrastructure Cyber Risk." *Coast Guard Proceedings*, vol. 71, no. 4 (2014–2015):42. http://uscgproceedings.epubxp.com/i/436751-win-2015.

nation is “to weaken, disrupt, or destroy.”[81] Although most nation states have the funding and resources to support whatever attack they deem necessary, ISC-CERT believes that will change within the next five to ten years.[82] Traditional terrorists do not play as great a role in the cyber realm because, according to Marshall Newberry of ICS-CERT, they "are less developed in their cyber capabilities than are other adversaries.”[83] Industrial spies and organized crime groups are out for profit and looking to put money in their or their company’s pockets. These spies or groups may work within the maritime industry itself, trying to get the upper hand on competitors. Hacktivists consist of groups who have a small political agenda. For example, Greenpeace could have hacktivists infiltrate an offshore oil platform to protest against oil drilling. Hackers make up the majority of cybercriminals today due to sheer size. What makes hackers unique is their ability to work almost anywhere and attack anything. Newberry states, “Most hackers do not have the level of skill required to threaten U.S. critical networks. … [W]ith the growing number of skilled and malicious hackers, the likelihood of successful attack continually increases.”[84]

The insider threat will be the worst one yet. According to Carnegie Mellon in 2012, an insider threat is “a current or former employee, contractor, or business partner who: has or had authorized access to an organization’s network, system, or data; can bypass existing physical and electronic security measure through legitimate measures.”[85] Insider threats are especially dangerous because they can happen for a number of different reasons. Greg Smith, an Intelligence Specialist Chief for U.S.C.G Cyber Command, states that reasons for insider threats can range from problems at work to divided loyalty, blackmail, compulsive behaviors, or issues with one’s family.[86]

---

81 ICS-CERT, “Cyber Threat Source Description,” accessed April 3, 2016, https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions#nat.

82 Ibid.

83 Newberry, “Maritime Critical Infrastructure Cyber Risk,” 42.

84 Ibid.

85 Greg Smith, “Combating Inside Threat: The greatest Threats are the Ones with Access,” *Coast Guard Proceedings* 71, no. 4 (2014–2015): 70, http://uscgproceedings.epubxp.com/i/436751-win-2015.

86 Ibid, 70.

The insider threat may be the most difficult to recognize or combat at a shipyard and terminal. Employers are hoping that their companies hire the right people for the job. However, there is a risk associated with hiring personnel—despite clear background checks—that makes any company, especially the maritime cyber domain, vulnerable. Chief Technology Officer of Imperva states, "For most organizations, insider threats have moved beyond risk into reality; however, many threat vectors can be protected against with a measured approach to business security."[87] Weaknesses in the maritime cyber domain and to our national security can be someone who knows a terminal very well and wants to cause direct or indirect harm to the country.

D. SERIOUSNESS OF A MARITIME CYBER-ATTACK

Recent events in the Maritime industry enable forecasters to predict the outcomes of maritime cyber-attacks in the United States. Port closures, union strikes, and delayed movements of ships can suggest how severe an attack could be on the nation. In this section, the aforementioned recent attacks and equipment vulnerabilities help create a scenario based on evidence.

1. Economic

The first major shutdown of a U.S. port since 1971 took place in September 2002 when the Pacific Maritime Association and the International Longshoreman and Warehouseman Union could not reach an agreement over pay. The closure of 29 ports on the West Coast lasted for 11 days with loss of revenues reaching $15.6 billion.[88] These port closures adversely affected rail and truck workers who move the cargo from a West-Coast port to the cargo's final destination. The port of Tacoma, which maintains supply routes for communities in Alaska, was unable to fulfill requisitions for supplies, which

87 Clinton Karr, "Mitigate Insider Threats With a Measured Approach to Security," *Reuters*, October 24, 2012, http://www.reuters.com/article/idUS146971+24-Oct-2012+HUG20121024.

88 Steve Goreman, "U.S. West Coast Ports Closed to Cargo Vessels Again for Weekend," *Reuters*, February 13, 2015, http://www.reuters.com/article/us-usa-ports-west-idUSKBN0LH2CK20150214.

cut off critical imports to the Last Frontier.[89] The loss of revenue and support of ships on the West Coast caused significant economic delays both directly for the country and indirectly for shipping companies who had contracts to meet and deliveries to make.

Again, in February 2015, the West Coast of the United States suffered 29 port closures because of a union strike, which essentially stopped the supply chain and routes of any cargo trying to enter or exit the United States. This port shut down took place not because of a cyber-attack but because 20,000 stevedores were working without a contract for more than six months.[90] Normal operations resumed after the union and the Pacific Maritime Association reached an agreement. Today, experts believe a similar shutdown of West-Coast port operations could lead to losses of $1–$2 billion daily.[91] These examples demonstrate how easily and quickly a stoppage at a major U.S. port can impact the nation's economy.

Hurricane Sandy hit the East Coast of the United States in 2012, devastating portions of New York and New Jersey. The impact of Hurricane Sandy caused $70 billion in damages to both commercial and privately owned businesses and homes.[92] The hurricane destroyed numerous terminal sensors including security cameras and control systems, power and telephone lines, and port infrastructure. Problems were widespread along the Eastern Seaboard of the United States as well as in the Caribbean as a majority of critical cargoes were either lost or unable to reach their final destinations.[93] Despite the devastation caused by Hurricane Sandy, terminal operations were able to resume safely

---

89 Kit Oldman, "Employers lock out Longshore Workers at West Coast Ports on September 27, 2002," *Historylink.org*, July 17, 2008, http://www.historylink.org/index.cfm?DisplayPage=output.cfm&file_id=8692.

90 Goreman, "U.S. West Coast Ports Closed."

91 Richard Kolko, "Countering the Maritime Cyber Threat," *Coast Guard Proceedings* 71, no. 56, (2014–2015): 50, http://uscgproceedings.epubxp.com/i/436751-win-2015; Steve Goreman, "U.S. West Coast Ports Closed to Cargo Vessels Again for Weekend," *Reuters*, February 13, 2015, http://www.reuters.com/article/us-usa-ports-west-idUSKBN0LH2CK20150214.

92 Linda A. Sturgis, Tiffany C. Smythe, and Andrew E. Tucci, "Port Recovery in the Aftermath of Hurricane Sandy: Improving Port Resiliency in the Era of Climate Change," Center for a New American Security, August 2014, 5, http://www.cnas.org/sites/default/files/publications-pdf/CNAS_HurricaneSandy_VoicesFromTheField.pdf.

93 Sturgis, Smythe, and Tucci, "Port Recovery in the Aftermath of Hurricane Sandy," 5.

when the Port Authority of New York and New Jersey began falling back on older technology. According to Mark Szakonyi, executive editor at Joc.com, mariners were able to restore somewhat normal operations using VHF radios, battle lanterns aboard tugs and storage facilities, as well as backup generators.[94] Substituting a cyber-attack for a disaster like Hurricane Sandy yields nearly the same impact, without the kinetic damage associated with a natural disaster. A cyber-attack will cause delays in operational commitments by ports. Cargoes will be lost in a cyber-world, and figuring out where everything is will be a logistical nightmare. The industry in New York and New Jersey were able to ease the burden of Hurricane Sandy with paper charts and VHF radios. New York and New Jersey have the capabilities in place to be more resilient against kinetic attacks, especially after 9/11. Backup charts and VHF radios will not be enough when a cyber-storm appears out of nowhere.

2. Liquefied Natural Gas

There are more associated risks than financial aspects of a maritime cyber-attack. Republican Representative Candice Miller from Michigan argues that liquefied natural gas (LNG) aboard ships and at terminal storage facilities will cause massive damage to surrounding communities and the environment if hacked.[95] The only accident in the United States from LNG happened in WWII when cells holding LNG ruptured, and one million gallons ended up in sewer pipes, killing 128 people and injuring 200 in Cleveland Ohio.[96] The likelihood of an event of this type resulting from a cyber-attack may seem remote, but the results of such an attack would cause economic, trade, and public safety concerns. Miller concluded her report to Congress, stating, "Just as we have hardened

---

[94] Mark Szakonyi, "U.S. Coast Guard takes lead to address cyber risks at ports," *JOC.com*, April 1, 2015, accessed April 3, 2016, http://www.joc.com/regulation-policy/transportation-policy/us-transportation-policy/us-coast-guard-takes-lead-address-cyber-risks-ports_20150401.html.

[95] John Bensalhia, "Cyber-attacks on U.S. Ports Risk Chemical Disaster," The Stack, Oct 12, 2015, https://thestack.com/security/2015/10/12/cyber-attacks-on-u-s-ports-risk-chemical-disaster/.

[96] Edward Dodge, "How Dangerous is LNG?" *Breaking Energy*, October 22, 2014, http://breakingenergy.com/2014/12/22/how-dangerous-is-lng/.

physical security, we need to do the same in the virtual space for systems critical to the marine transportation system to protect against malicious actors."[97]

E. SUMMARY

Attacks on the maritime community are all significant in helping determine whether more measures, programs, and government agencies need to be involved in protecting the maritime community against an attack. A serious attack on the United States could be devastating economically, not to mention deadly. In the end, the evidence provided in this chapter strongly suggests that maritime networks and equipment are vulnerable to a cyber-attack.

[97] Pierluigi Paganini, "U.S. Ports Are Still Vulnerable to Cyber-attacks That Release Dangerous Chemicals, Cybersecurity in the Maritime Industry is Crucial for Homeland Security." *Security Affairs*, October 12, 2015, http://securityaffairs.co/wordpress/40960/security/us-ports-vulnerable-hacking.html.

III. NATIONAL SECURITY AND MARITIME CYBER WARFARE

> We are vulnerable in the military and in our governments, but I think we're most vulnerable to cyber attacks commercially. This challenge is going to significantly increase. It's not going to go away.
>
> —Admiral Michael Mullen, USN[98]

Maritime cyber-attacks have happened in the past, are happening now, and will continue in the future. The more today's mariners, ship brokers, husbandry agencies, and others surrounding the community rely on Internet-based programs to assist and ease tasking, the more the community will be vulnerable to attacks. To evaluate the readiness of U.S. ports to cyber threats, Commander Joseph Kramek, a USCG Federal Executive Fellow for Brookings, conducted a series of port vulnerability assessments in top U.S. ports. This assessment provided data for Kramek's understanding of how well prepared the United States is for an attack. In his preface, Kramek states, "The level of cybersecurity awareness and culture in U.S. port facilities is relatively low…and not a single one [port] had developed a cyber incident response plan."[99]

A maritime cyber-attack at a major port in the United States would disrupt the numerous operations of the port, cause financial burdens, and make U.S. infrastructure vulnerable. To determine whether a maritime cyber-attack from a non–U.S.–flagged vessel entering the United States poses a threat to U.S. national security, this chapter evaluates evidence from Kramek's assessments of the Port of Baltimore, Port of Houston Authority, Ports of Long Beach and Los Angeles, Port of Vicksburg, and the Port of Beaumont. Second, this chapter analyzes the cybersecurity culture in these ports. Finally, this chapter summarizes the report, stressing the importance for maritime cyber dominance.

---

98 Geoff Colvin, "Adm. Mike Mullen: Debt Is Still Biggest Threat to U.S. Security," *Fortune*, May 10, 2012, http://fortune.com/2012/05/10/adm-mike-mullen-debt-is-still-biggest-threat-to-u-s-security/.

99 Joseph Kramek, "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities. "*Foreign Policy at Brookings*, (2013): vii, http://www.brookings.edu/research/papers/2013/07/03-cyber-ports-security-kramek.

A. FUNDING AND PORT ANALYSIS

Funding is always required for the implementation of security measures. Government agencies provide part of the funding for the maritime community to promote security and safety at U.S. ports. Port management often uses the money based on threat evaluations as top officials deem necessary. This section evaluates port funding and the overall cybersecurity resilience of top ports in the United States.

1. U.S. Port Funding

The attacks of September 11 reminded the United States that oceans no longer protect the U.S. from deliberate attacks. In 2002, the Maritime Transportation and Security Act (MTSA) was signed into law by Congress to directly support port and waterway security.[100] Under § 70107, Grants, of the MTSA, the following funding is outlined:

> Salary, benefits, overtime compensation, retirement contributions, and other costs of additional Coast Guard mandated security personnel.
>
> The cost of acquisition, operation, and maintenance of security equipment or facilities to be used for security monitoring and recording, security gates and fencing, marine barriers for designated security zones, security-related lighting systems, remote surveillance, concealed video systems, security vessels, and other security-related infrastructure or equipment that contributes to the overall security of passengers, cargo, or crewmembers.
>
> The cost of screening equipment, including equipment that detects weapons of mass-destruction and conventional explosives and of testing and evaluating such equipment, to certify secure systems of transportation.
>
> The cost of conducting vulnerability assessments to evaluate and make recommendations with respect to security.[101]

---

[100] Maritime Transportation Security Act of 2002, Public Law 107-295, Nov. 25, 2002. https://www.gpo.gov/fdsys/pkg/PLAW-107publ295/pdf/PLAW-107publ295.pdf.

[101] Ibid.

The effort to meet requirements set by MTSA 2002 is supplemented through the Federal Emergency Management Agency (FEMA), which issues grants from the Port Security Grant Program (PSGP).[102] FEMA developed a risk-analysis model to categorize port areas in the United States as one of three categories—Group one, Group two, or Group three—in order to issue appropriate funds. Group one contains the highest risk ports and includes, Los Angles, Long Beach, and Houston. Group two includes Baltimore, Beaumont, and Vicksburg. Kramek's report did not evaluate ports in group three.[103] Since Kramek's study focuses on fiscal year (FY) 2012 funding of PSGP monies, this chapter uses the total funding of FY2012, $97.5 million.[104] MTSA 2002 does not list cybersecurity as a threat.

2. Maryland Port Administration and the Port of Baltimore

The Port of Baltimore (POB) is a crucial hub for goods and services crossing the Atlantic Ocean to the United States. According to World Port Source, in 2015 the POB received more than 13.3 billion kilograms of imports from more than 125 countries, and the Maryland Port Administration (MPA) managed 46,827 TEUs. The volume of business the port sees is critical to the surrounding population for direct economic reasons, trade, and employment. The POB has direct access to rail systems and highways, which make it easy to deliver goods throughout the country.

The POB piers are owned by the MPA; however, Ports America Chesapeake (PAC), which rents the space from MPA, takes full charge of the offloading process. The process begins with computer and terminal management systems that manage automatic crane operations prioritizing TEUs for transportation. While the automatic offloading process continues, stevedores and PAC officials manage the operations from wireless network devices, ensuring accuracy during the offloading process. Many of the devices used to verify TEU placement are third-party handheld scanners. While PAC rents the

---

[102] Kramek, "The Critical Infrastructure Gap," 9.

[103] Ibid.

[104] Federal Emergency Management Agency (FEMA). "FY 2012 Port Security Grant Program (PSGP)." Last accessed, March 26, 2016. https://www.fema.gov/fy-2012-port-security-grant-program.

space from the MPA, MPA has zero insight or validation authority over cybersecurity in any of the network terminals, scanners, or computers used by PAC. Although the process is efficient in turnaround time, the logistic management system and networks in place are vulnerable to cyber-attack.

MPA does control who accesses the facility from roadways but not through a physical security guard at a gate. In order to maintain efficient vehicle movement in and out of the port area, MPA has employed a software program known as eModal, described on their website as follows:

> [The] world's largest port community system … used extensively throughout North America. As a cloud based solution, eModal offers intermodal supply chain stakeholders complete visibility via a central portal. eModal enables users to manage truck registries, appointments, dispatching, chassis rental billing and fee payments.[105]

Once registered on MPA's website for eModal, truckers are given a radio frequency identification tag (RFID), which identifies the truck and driver. While the trucks move through entry points and toward terminals, MPA watches the activities of the port from video monitors with more than 400 security cameras throughout the POB. eModal's network is managed by the MPA's in-house information-technology (IT) support team. Although the IT members can record and save all data from eModal and security cameras onto a shared network with the Maryland Department of Transportation (MDOT), they cannot access or monitor data from PAC.[106]

The MPA has reported numerous outside attempts to gain access to eModal and the security cameras over the installation. It attributes these threats to crewmembers of ships entering the port who try to access the Wi-Fi connection. The ability to narrow down the source of cyber-attacks is difficult because the MPA is unable to access all electronic systems and networks managed either by PAC or from commercial shipping. Security officers at the MPA have installed firewalls and malware protection to detect, deter, and prevent such attacks from seriously shutting down the port. Kramek states, "A

---

105 eModal. Last accessed: March22, 2016. http://welcome.emodal.com/.

106 Kramek, "The Critical Infrastructure Gap," 12.

disruption to any of MPA's or its terminal lessees' networked system would quickly disrupt cargo operation and slowly ripple out to impact the one-third of the U.S. population that resides within an overnight drive of POB."[107] Furthermore, the lack of concern from upper-management over maritime cyber-security has left the MPA with insufficient knowledge and training for cyber-threats.[108] MPA did not have a cybersecurity mitigation plan or a pre-planned response if a cyber-attack were to take place at the POB despite the amount of services the port handles. The report mentions that the POB has focused its security efforts on physical security by adding cameras and an access-control center for visitors; nevertheless, the POB has never requested funding for cyber-related protection.[109]

In response to acquisitions in the report, POB spokesman Richard Scher claims the report was "misleading and factually incorrect" and that the POB has worked very closely with FBI's cyber security team at Fort Meade, Maryland.[110] Because Kramek's study was not sanctioned by a governing authority, Scher would not reveal details about the POB's cyber-security protocols but insisted they were up to date.[111]

In its Strategic Plan 2015, the MPA states,

> The MPA has incorporated policies, procedures and technology which exceed the Act's requirements. The MPA continuously assesses the potential threats and vulnerabilities of its terminals in order to maintain the highest level of security possible.[112]

---

[107] Kramek, "The Critical Infrastructure Gap," 13.

[108] Ibid.

[109] Ibid.

[110] Candy Thomson, "Port of Baltimore is Vulnerable to Cyber-attack, Brookings Study Says." The Baltimore Sun. July 05, 2013. http://articles.baltimoresun.com/2013–07–05/business/bs-bz-port-security-20130703_1_maryland-port-administration-cybersecurity-port-officials.

[111] Ibid.

[112] Maryland Port Administration, "Strategic Plan 2015." September 2015. 22. http://www.mpa.maryland.gov/_media/client/planning/Strategic__Plan%202015.pdf.

Despite these claims, the word "cyber" appears only once in the 36-page document, suggesting that the MPA still does not take a maritime cyber threat seriously.[113] No other information regarding cyber measures taken by PAC could be found on its website.

3. Port of Houston

The Port of Houston (POH) is the largest port in the United States and the tenth largest in the world, located inland off the Gulf of Mexico. In 2013, the POH received 77.6 million tons of cargo with a net worth of $74.3 billion. The port's biggest importers by tonnage include Mexico, Russia, Saudi Arabia, Iraq, and Columbia.[114] Port capacity comprises 44 general cargo wharves, 19 container wharves, five liquid bulk wharves, and three dry bulk wharves with more than 150 auxiliary port facilities.[115] The port operations are controlled by the Port of Houston Authority (PHA), which owns eight terminals and leases the terminals as needed.

The PHA relies on a terminal operating system known as NAVIS. NAVIS controls crane operations, security, cargo movements, billing, automotive gates, fuel farms, and HVAC systems at the facility.[116] NAVIS appeals to more than 280 terminal centers worldwide due to its simplicity for port operations.[117]

The physical security of the POH is high, with three different agencies responsible: the Houston Ship Channel Security District (HSCSD), the Houston Police, and the USCG. All are equally invested in the safety of navigation and maritime presence in and out of the port. The PHA has an in-house IT team that monitors the networks controlling port operations. The PHA has a software system and firewalls in place to monitor the port's cyber realm. To analyze the effectiveness of the software and firewalls in place, the PHA hired third-party contractors to conduct a series of "penetration testing"

---

[113] Maryland Port Administration, "Strategic Plan 2015."

[114] Port of Houston Foreign Trade Statistics, Last accessed March 22, 2016. http://www.portofhouston.com/static/gen/inside-the-port/Communications/Factsheets/FTS_Tonnage_Cargo_2013.pdf.

[115] The Port of Houston, Last accessed March 22, 2016. http://www.portofhouston.com/.

[116] Kramek, "The Critical Infrastructure Gap," 14.

[117] Navis.com, "About NAVIS N4." Last accessed, March 26, 2016. http://navis.com/get-more-n4.

attacks on the network.[118] Despite the red-team's analysis that demonstrated IT was able to fix potential threats before they became catastrophic, Kramek found multiple weaknesses in the PHA: "New employees do not receive cybersecurity training before being granted network access, and private stevedore company employees hired by PHA to conduct cargo operations use their own laptops to connect to PHA's cargo management system."[119] Furthermore, PHA "did not cite cybersecurity as one of its top three challenges or threats," despite worries from the PHA's IT staff over the use of personal thumb drives. The ability for stevedores to access the cargo management system on personal computers threatens PHA's networks.

The PHA's Strategic Plan for 2015, prepared by global management consulting firm Leigh Fisher, did not list "cyber" anywhere in the port's plan. Threats therein include "events—natural disasters, security incidents, [and] accidents."[120]Although the term "security incidents" could possibly include cyber threats, the report does not specifically spell out cyber concerns, thus pointing to the lack of seriousness in the way port leadership approaches the maritime domain. In his conclusion, Kramek states, "If the NAVIS system were to go down, PHA's terminal operations would cease. A cyberattack …would be catastrophic … impacting 70 percent of all containerized cargo … as well as a large portion of the American energy supply."[121]

4. The Ports of Los Angeles and Long Beach

The two largest ports on the West Coast of the United States are the Ports of Los Angeles (PLA) and Long Beach (PLB). Both ports accept goods daily from major exporting countries like China, Vietnam, and Malaysia. In 2015, PLA's and PLB's TEU counts were 8.2 and 8.7 million, respectively, making up more than 15 million TEUs in

---

118 Kramek, "The Critical Infrastructure Gap," 14.

119 Ibid.

120 Leigh Fisher, "Strategic Plan Presentation Prepared for The Port of Houston Authority." April 28, 2015. http://www.portofhouston.com/static/gen/inside-the-port/Strategic%20Planning/PHA_Strategic_Plan_Approved_2015–0428_(FINAL).pdf.

121 Kramek, "The Critical Infrastructure Gap," 16.

2015 alone for the terminals to manage.[122] The service capabilities for both of these ports include containerized, dry bulk, liquid bulk, break bulk, and roll-on/roll-off (RO-RO) capabilities. Due to the shallow drafts of California ports, many supertankers, including very large crude carriers (VLCCs) must make berth in either PLA or PLB to offload cargo.

PLB relies on major computer-based networks to ensure smooth and efficient terminal operations. These networks include control systems, which manage the offloading of crude oil, crane operations employed by stevedores, logistics management software, and container management software.[123] Due to the vast amount of cargo operations surrounding the port, PLB understands that a major network is required to monitor every aspect of operations within the limits of the PLB. In 2009, the PLB as well as more than 25 federal, state, and local agencies working together to support port security formed a joint command and control center (JCCC) to establish a common operating picture. PLB maintains a highly trained in-house IT department, which works on network issues and, when necessary, outsources contractors to support the IT department.[124]

In order to maintain its effectiveness, the port developed the Virtual Port System (VPS), which came online in the summer of 2014.[125] VPS has the ability, according to the Port of Long Beach, to "integrate information from more than 50 data sources into comprehensive real-time images the agencies can access simultaneously to coordinate and deploy response teams, tackle the problem and restore port operations faster and

---

[122]The Port of Los Angeles, Last accessed March 23, 2016. https://www.portoflosangeles.org/maritime/stats.asp; The Port of Long Beach. Last accessed March 23, 2016. http://www.polb.com/economics/stats/yearly_teus.asp.

[123] Kramek, "The Critical Infrastructure Gap," 17.

[124] "Port of Long Beach Strategic Plan 2016." Last accessed March 29, 2016. 12. http://www.polb.com/civica/filebank/blobdload.asp?BlobID=12848.

[125] Kramek, "The Critical Infrastructure Gap," 18.

more efficiently than ever before."[126] VPS creates a common operating picture for the PLB and all 26 of the entities involved.

PLB is aware that the port and its network infrastructure are at risk, and as a precautionary measure, the port did not allow outside users to access the Internet or Wi-Fi at the port. As of 2013, PLB had invested over $1 million in network infrastructure including firewalls and security applications that monitor all users on the network. Kramek assesses the PLB as follows: "The second busiest port in the nation does not currently have a dedicated written cybersecurity directive or response plan, nor is cybersecurity response part of any existing risk management plans."[127] Upon completion of the initial assessment, the PLB reported that it had completed a vulnerability assessment on VTS prior to installation. No other concerns were listed.[128]

The research and proactive approach by the PLB did not end after the assessment from Kramek. On October 8, 2015, Randy Parsons, Director of Security Service at the Port of Long Beach, presented written testimony to the House Committee on Homeland Security's Subcommittee on Border and Maritime Security, voicing his concerns to members of Congress. In his written statement, Parsons noted that maritime cyber-attacks could affect the PLB as well as have secondary and tertiary effects on subcontractors including "shippers, vessels, terminal operating systems, equipment, storage facilities, rail and truck."[129] Proving the vulnerability of the nation's ports against cyber-attacks, Parsons admits that the PLB receives "one million hacking attempts a day."[130] In his testimony to Congress, Parsons outlined recommendations and actions he believed would

---

126 The Port of Long Beach, Last accessed March 23, 2016. http://www.polb.com/economics/stats/yearly_teus.asp.

127 Kramek, "The Critical Infrastructure Gap," 18.

128 Ibid.

129 *Protecting Maritime Facilities in the 21st Century: Are Our Nation's Ports at Risk for a Cyber Attack? Hearing before the House Committee on Homeland Security Subcommittee on Border and Maritime Security*(October 8, 2015) (statement of Randy Parsons, Director of Security Services Port of Long Beach), http://docs.house.gov/meetings/HM/HM11/20151008/104007/HHRG-114-HM11-Wstate-ParsonsR-20151008.pdf.

130 Ibid.

create a more resilient maritime community. These recommendations are evaluated in Chapter V.

The PLB is adjacent to the PLA, the largest port in the western United States. During the port review in 2013, the PLA believed it was susceptible to maritime cyber-attacks because of the port's reliance on logistic management systems and the amount of lessees the PLB accepts.[131] PLA focuses a majority of funding toward physical security because of the number of small and recreational craft in the area, which continues to be a concern for security managers at the port.

The PLA established a geographic information center that enables real-time alerts for which all parties concerned at the PLA can monitor activities of the port. The PLA has an in-house IT department that monitors networks and servers as well as ensures the networks are "routinely backed up."[132] The IT department is responsible for not only the networks and domains but also the training of all new employees who work for the PLA on cyber issues and awareness. The IT department runs software and network scans that look for potential hacking attempts on the network. Unfortunately, at the time of the study, the PLA "ha[d] not conducted a cybersecurity vulnerability assessment nor … ha[d] a cyber incident response plan," though it had received $1.65 million for bulking up cybersecurity awareness and defense.[133] Kramek's report concluded that the security manager of the PLA during a cyber-attack would only be informed of the impacts to the port, leaving the in-house IT team to fix the mess.[134]

On October 16, 2013, the PLA requested funding for the first phase of a cyber security operations center (CSCO).[135] The CSCO concept had been floating around security managers since early 2009, and with the rise of cybercrimes, it was crucial the PLA moved ahead with the program. The total cost for the CSCO project was

---

131 Kramek, "The Critical Infrastructure Gap," 18.

132 Ibid, 19.

133 Ibid.

134 Ibid.

135 Sara Scullin, "Order in the Port." Law Enforcement Technology. April 2015, 27. http://let.epubxp.com/i/488815-apr-2015/26.

$2,564,000, of which $1.6 million came from PSGP's 2012 funds and the remainder from PLA dividends. The reported net cost for operating the CSCO is $50,000 per year.[136]

Detailed reports highlight the capabilities of the CSCO, including "advanced hardware and software that is used to proactively monitor the computer environment to prevent a breach and be able to quickly detect and respond if a breach does occur."[137] According to the CSCO, over the past few years, the program "has reduced the cyber risks for the Port of LA by complementing its exciting cyber efforts with improved cyber defense and response, and data analysis and sharing."[138] In November 2014, the PLA won the American Association of Port Authorities' (AAPA's) 2014 Information Technology Award for the development and utilization of the CSCO.[139] PLA appears to be on the right path toward maritime cyber resilience.

5. Port of Vicksburg

As the Mississippi River flows into the Gulf of Mexico, the Port of Vicksburg (POV) is decisive for open sea-lanes into the heart of the United States. The Warren County Port Commission, in charge of port operations at the POV states, "The Vicksburg Port services industries that range from steel and lumber, to coal and petroleum … with a customer base spanning from small-businesses to Fortune 500 Companies."[140] Providing cost effective transportation inland, the POV sees 900,000 tons of goods a year, which eventually end up on trucks, rail, or smaller shipping vessels headed up the Mississippi. The POV is a crude-oil hub for the Gulf of Mexico and refineries located at Ergon's St

---

136 Executive Directors Report to the Board of Harbor Commissioners. "Resolution NO.___ - Agreement Between the City of Los Angeles Harbor Department and Accuvant, Inc. For a Cyber Security Operations Center Phase 1." The Port of Los Angeles. October 16, 2013. 4–5. https://www.portoflosangeles.org/Board/2013/November%202013/110713_Item_15_Board_Report.pdf .

137 "Cyber Security Operations Center 2014 AAPA Information Technology Award Application Summary." The Port of Los Angeles. Last accessed March 23, 2016. http://aapa.files.cms-plus.com/Port%20of%20LA%20SUMMARY%20-%202014%20AAPA%20IT%20Award.pdf.

138 Ibid.

139 Phillip Sanfield, "Port of Los Angeles Earns 18 Awards for Cyber Security Operations Center, Communication Initiatives." Port of Los Angeles. November 24, 2014. https://www.portoflosangeles.org/newsroom/2014_releases/news_112414_AAPA_Awards.asp.

140 Warren County Port Commission, Last accessed March 23, 2016. http://vicksubrgedf.org/.

James terminal. Ergon Refining, Incorporated (ERI) and Magnolia Marine Transport (MMT) share joint logistic management software, which manages cargo offloading, secondary transportation, storage capacity, and terminal operations.[141]

The software used to process logistic data on computers at ERI and aboard tugs is susceptible to hacking. In an effort to cut overhead costs, ERI purchased a license for data acquisition program Supervisory Control and Data Acquisition (SCADA). SCADA manages many of the terminal's operations including the valves, pipelines, and remotely controlled services within the port.[142] SCADA made headlines when it admitted that cyber-attacks against its server increased from 163,228 in 2012 to 675,186 as of January 2014. The attacks targeted critical infrastructure, power plants, factories, and refineries in Finland, the United Kingdom, and the United States.[143] *Homeland Security Today*'s Senior Editor Amanda Vicinanzo reviewed the cyber-attacks associated with SCADA, stating, "SCADA attacks often go unreported, since companies are only required to report security breaches involving personal or payment information. Consequently, individual companies may be unaware a SCADA threat exists until they are targeted themselves."[144]

The port's IT security operations tended to be weaker at the time of the report compared to the POB, PLA, and PLB. Kramek concluded that ERI was somewhat aware of cyber threats in the maritime community. MMT was "not as aware of cybersecurity challenges, mainly because very few networked systems exist on its vessels other than the laptops running cargo tracking and vessel location systems."[145] The report reveals four findings: only one individual was responsible for cybersecurity at ERI; regular users of SCADA never received cyber awareness training; cybersecurity vulnerability assessments were never completed; and preplanned responses had not been established to

---

141 Warren County Port Commission, Last accessed March 23, 2016. http://vicksubrgedf.org/.

142 Kramek, "The Critical Infrastructure Gap," 21.

143 Mike Lennon, "Attacks Against SCADA Systems Doubled in 2014: Dell. Security Week. April 13, 2015. http://www.securityweek.com/attacks-against-scada-systems-doubled-2014-dell;%20A.

144 Amanda Vicinanzo, "Cyber Attacks Against SCADA Systems Doubled in 2014, Says Dell Threat Report." Homeland Security Today. April 14, 2015. http://www.hstoday.us/single-article/cyber-attacks-against-scada-systems-doubled-in-2014-says-dell-threat-report/ae81a11c6c44f731bfd5ff8ab6f26c88.html.

145 Kramek, "The Critical Infrastructure Gap," 21–22.

respond to a cyber-attack.[146] Kramek's study mentions that ERI had been working toward developing a cybersecurity risk plan and strategies that incorporate cooperative measurements between the company and contractors. Furthermore, there was no searchable strategic plan for POV nor did the POV take the maritime cyber threat seriously as of 2013.

6. The Port of Beaumont

The Port of Beaumont (PBM) is located in Texas on the Gulf of Mexico, offering 600,000 square feet of storage; access to rail, major highways, and the Gulf Intercostal Waterway; and provides services for military and commercial usage.[147] Recognized by the U.S military's Transportation Command as the busiest military port in the world, "a cyber disruption here would impact almost 50 percent of all military cargo bound for overseas contingency operations and impact the U.S. military's ability to respond to crisis or conflict."[148] The United States Navy Ship (USNS) *Red Cloud* (T-AKR-313), home-ported out of the PBM, is one of the Military Sea Lift Command's largest preposition army stock ships. The purpose of the *Red Cloud* and the other seven ships in her class is to carry a majority of operational equipment and supplies to support operations overseas. In conjunction with the USNS *Red Cloud*, the U.S. Army's 842nd Transportation Battalion along with civilian contractors support military loading and logistical operations at the POV. Like its civilian logistics agencies, the 842nd uses a complex network for logistical services known as a logistics management system (LMS).

The PBM cited potential waterborne threats against USNS shipping among the top security concerns for the port. Port networks are stand-alone systems managed by 40 IT civilian staff-members with one team member who is responsible for cybersecurity. Kramek's study noted, "PMB has not conducted a cybersecurity vulnerability assessment

---

146 Kramek, "The Critical Infrastructure Gap," 22.

147 Port of Beaumont, "Our Facilities." Last accessed March 25, 2016. http://www.portofbeaumont.com/.

148 Kramek, "The Critical Infrastructure Gap," 23.

of its network," and none of the IT department's members or new employees received any sort of information-assurance training or follow-up during in-processing.[149]

In order to spot-check the 842nd, U.S. Transportation Command (USTRANSCOM) conducted its own cybersecurity vulnerability. According to Kramek, the "842nd ha[d] dedicated cyber incident instructions that set forth specific actions to take in the event of a cyber disruption or attack" in which the military members were trained specifically to handle a network intrusion.[150] Overall, the report highlighted how little concern the POV, with the exception of the 842nd, had for network security issues, despite known vulnerabilities.

B. WHAT DOES THIS MEAN FOR U.S. PORTS?

The overall focus of the ports listed in 2013 was physical security. Sharing the ports with civilian pleasure craft and fears over waterside attacks concerned the port security managers the most. In his analysis of maritime cybersecurity, Kramek states: "Not only is cybersecurity awareness in U.S. port facilities generally low, but the cybersecurity culture in U.S. port facilities is generally lacking."[151] Among the ports, very few spent PSGP funds for cybersecurity projects as of FY2012, as shown in Table 1.[152]

149 Kramek, "The Critical Infrastructure Gap," 24.

150 Ibid, 25.

151 Ibid, 27.

152 Ibid.

Table 1. Kramek's Overview of PSGP Monies [153]

Group Type	Port	Vulnerability Assessment	Written Response Plan	PSGP Monies Received Since 2007	Use of PSGP for Cybersecurity Project
Group I	Port of Houston	No	No	$40,368,962	$0
	Port of Long Beach	Yes	No	$120,000,000 (since 2001)	$800,000 (indirect)
	Port of Los Angeles	No	No	$40,593,367.97	$1,650,000
Group II	Port of Baltimore	No	No	$6,903,292	$0
	Port of Beaumont	No	No	$0	$0
	Port of Vicksburg-Ergon	No	No	$0	$0
N/A	842nd Transportation Command - Beaumont	Yes	Yes	N/A	N/A

Kramek's study highlights some interesting cost-analysis numbers. The PLB conducted a vulnerability assessment on its own with a reported cost of $30,000. Using the checklist that the PLB used to conduct its assessment as a baseline for future vulnerability assessments, all 33 ports in Group one could have completed a vulnerability assessment for under $1 million or 1.03 percent of the FY2012 budget. Kramek hits the point home: "The cost of conducting cyber vulnerability assessments appears to be relatively low compared to the costs of a successful attack."[154]

FY2015 and FY2016 both saw allowances for $100 million, according to FEMA's allowance for PSGP funds. DHS's Port Security Grant Program directive in FY2016 focuses spending on "supporting increased port-wide maritime security risk management; enhancing maritime domain awareness; supporting maritime security training and exercises; and maintaining or reestablishing maritime security mitigation

[153] Source: Kramek, "The Critical Infrastructure Gap," 27.

[154] Ibid, 28.

protocols."[155] The directive stresses that monies from the fund should be used toward maritime domain awareness though nowhere does it say how much or what percentage of monies should be used toward this purpose.

C. EUROPEAN UNION MARITIME CYBERSECURITY COMPARISON

The European Union (EU) has similar issues in cybersecurity like the United States. In 2010, The Digital Agenda for Europe promoted the unification of maritime cybersecurity to the EU by "focusing on prevention, preparedness and awareness, as well as develop effective and coordinated mechanisms to respond to new and increasingly sophisticated forms of cyberattacks and cyber-crime."[156] In 2011, the European Network and Information Security Agency (ENISA) conducted an analysis on member states' cybersecurity in a report called *Analysis of Cyber Security Aspects in the Maritime Sector*. The purpose of ENISA is to develop working relationships with the EU and member states while making best practices available for information systems and networks building resilience and security.[157]

The maritime community in the EU is very similar to that of the United States in complexity, overall size, and dependence on open maritime facilities. Member states comprise 28 independent nations, 23 of which border waterways. Altogether, member states have 1,200 commercial and industrial ports with more than 8,100 flagged vessels, making up 30 percent of the world's shipping, and 40 percent of trade among member states travels through sea-lanes.[158]

---

155 Federal Emergency Management Agency (FEMA). "Fiscal Year (FY 2016) Port Security Grant Program (PSGP) Fact Sheet. Last accessed March 26, 2016. https://www.fema.gov/media-library/assets/documents/114444.

156 "Analysis of Cyber Security Aspects in the Maritime Sector," European Network and Information Security Agency (ENISA), November 2011, 4, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts/cyber-security-aspects-in-the-maritime-sector 1/at_download/fullReport+&cd=1&hl=en&ct=clnk&gl.

157 Ibid.

158 "The EU Maritime Security Strategy and Action Plan Information Toolkit." European External Action, last accessed April 20, 2016, 2. http://eeas.europa.eu/maritime_security/docs/maritime-security-information-toolkit_en.pdf.

Similar to Kramek's findings in his report on U.S. port cybersecurity, the EU maritime industry as a whole has little awareness about maritime cybersecurity and the potential threats or actors aimed at disrupting EU supply chains. ENISA's findings suggest that the EU maritime community has an incomplete understanding of the cyber threat, a lack of expertise in ICS systems and networks, security managers who maintain ad hoc protocols and responses to cyber-attacks, and little incentives or direct economic support from member-state governments.[159] Like CyberKeel, ENISA admits, "Insufficient awareness and focus on cyber security results in a low sense-of-urgency combined with an inadequate preparedness regarding cyber risks."[160]

ENISA's report provides evidence that maritime players in the EU are becoming more dependent on IT systems, and the lack of knowledge surrounding cyber threats is poor.[161] Terminal operators establish Internet connectivity with information and communications technology (ICT) systems that require no connection to the Internet. Those systems connected to the Internet have little anti-virus protection or software providing forceful backup to the operators against cyber threats. Resiliency in maritime cybersecurity in the EU requires a joint strategy that requires all member states to adopt common goals in strengthening networks. According to ENISA, "Lack of coordination between stakeholders … (European and national) brings major discrepancies in the way maritime security is addressed."[162] The complexity of having multiple parties involved with cybersecurity and port operations is reflected through Kramek's study of ports in the United States. Many of the issues visible in ENISA's 2011 report and reflected in Kramek's study show the international maritime community is at risk, thus putting the United States' national security at greater risk.

159 "Analysis of Cyber Security Aspects," ENISA, 9–18.

160 Ibid, 8.

161 Ibid.

162 Ibid, 11.

D. SUMMARY

Kramek's study was the first open-source cybersecurity vulnerability assessment of its time. For years, security managers in U.S. port facilities placed maritime cybersecurity training and planning on the backburner. The approaches from all five facilities had different staffs, programs, and software, as well as placed the responsibility at different levels. Evidence from the study shows, with the exception of the 842nd, not one single port as of 2013 had developed or even thought about a preplanned response or the after math of a cyber-attack.

Upon its completion, some ports accepted the assessment as a warning and took advantage of funding opportunities to develop cybersecurity awareness programs. Although the amount of information provided in the study analyzes five specific U.S. ports, these ports are the bread and butter of American commerce and energy. Although positive steps have been made in some U.S. ports, not all of the ports have the same funding or perspective on maritime cybersecurity. In the end, potential attackers do not discriminate over who has funding, who has developed a preplanned response, or who is responsible for maintaining a secure network.

According to the most recent studies, the EU and the United States have insecure maritime cyber domains. ENISA's concerns over internal maritime cyber security reflect issues that impact U.S. national security. Maritime cybersecurity starts before a foreign ship enters a U.S. port, and the international community must work together to protect one another.

IV. CYBERSECURITY AND RESPONSIBILITY

> I fully expect that during my tenure as commander of the U.S. Cyber Command there will be offensive activity directed against critical infrastructure of the United States designed to damage, destroy, or manipulate.
>
> —Admiral Mike Rodgers, U.S. Cyber Command[163]

Citizens of the United States should feel a sense of security in the face of foreign threats because of the layers of defense the United States has developed to thwart potential aggressors. Federal, state, and local authorities all have certain responsibilities for maintaining a safe world to live in while maintaining routine operations in the realm of physical security, once a wall is penetrated; someone notices the breach and responds to the threat. The cyber community is much different. Although the federal, state, and local authorities have a role in physical security based on laws of the land, it is unclear how capable or willing these agencies are to deter and respond to cyber threats.

First, this chapter examines the USCG's responsibilities for maritime cybersecurity in the United States. Second, it reviews other supporting authorities of maritime cybersecurity. Third, it reviews the European Union (EU)'s cybersecurity policies. Fourth, it compares the EU's cybersecurity program to that of United States through a real-life scenario. Finally, it compares the cybersecurity responsibilities of the United States and the EU.

A. UNITED STATES COAST GUARD CYBER OPERATIONS

Under PPD 21, the USCG is granted the authority and responsibility of the maritime transportation sector as it pertains to cybersecurity. To address different aspects of the cyber realm and players in the maritime community in the United States, the

163 Joseph Menn, and Warren Strobel, "New NSA Chief Vows More Transparency for Embattled Agency," *Reuters*. May 12, 2014. http://www.reuters.com/article/us-cyber-summit-nsa-rogers-idUSBREA4B0XU20140512.

National Infrastructure Protection Plan (NIPP) appoints the Coast Guard in charge of defending the Marine Transportation System (MTS) from all cyber threats. The Coast Guard Office of Port and Facility Compliance (CG-FAC) is the lead agency for marine transportation system (MTS) cyber-security. The United States Maritime Administration (MARAD) defines MTS as "waterways, ports, and inter-modal land-side connections that allow the various modes of transportation to move people and goods to, from, and on the water."[164] CG-FAC "serves as the Executive Secretariat representing the CG as the Sector Specific Agency for the Maritime Mode within the larger transportation Systems Sector. …CG-FAC will provide policy and guidance … to establish a consistent and effective approach to cybersecurity."[165] In January 2015, CG-FAC invited members of the maritime community to a meeting to discuss new projects pertaining to maritime cybersecurity. The meeting, held in Washington, D.C., had representatives from the USCG's, vessel operators, academics, port operators, and others with joint interests in the MST. CG-FAC also leads the Protect Infrastructure Cyber Strategy Implementation Team (CSITT), which consists of members from all over the Coast Guard in direct support of maritime cybersecurity. CG-FAC put pressure on the International Maritime Organization (IMO) to work in unison with the maritime community to maintain overall resilience. CG-FAC sends out monthly notices to the maritime community in the United States with links to cybersecurity awareness bulletins, training, tools, and alerts. CF-FAC continues to promote policy development, training, resource allocation, and research in the maritime cyber sector. [166]

The USCG adapted three cyber security priorities in its 2015 *Cyber Security Strategy*: defending cyberspace, enabling operations, and protecting infrastructure. The Coast Guard, while working with other partners in cyber defense in the United States,

---

164 United States Maritime Administration, "Marine Transportation System (MTS)." Last accessed April 9, 2016. http://www.marad.dot.gov/ports/marine-transportation-system-mts/.

165 "Cyber Security and the Marine Transportation System." Commandant of the Coast Guard Message Traffic. Aug 02, 2013. http://www.uscg.mil/announcements/alcoast/323–13_alcoast2.txt.

166 Ibid.

utilizes its intelligence teams to collect and analyze data that pertains to potential cyber-attacks on the Coast Guard or the MTS.

1. Defending Cyberspace

The first priority of the Coast Guard is to defend cyberspace from potential adversaries. To meet this objective, the Coast Guard lists three specific goals: to "identify and harden systems and networks, understand and counter cyber threats, and increase operational resilience."[167] The Coast Guard makes use of its resources to manage the cyber threat in the United States through gathering intelligence, developing partnerships with sister agencies, monitoring system networks, improving training- and technology-based focus groups, updating facilities with the most recent threat postures, and creating mitigation plans. Defending cyberspace for Coast Guard systems and the MTS is extremely difficult and requires joint support of Department of Homeland Security (DHS) and Department of Defense (DOD) assets. Coast Guard is working toward partnerships with customs and border protection, customs enforcement, immigration, the Federal Bureau of Investigation (FBI), and the Department of Energy.[168] Sharing best practices among different federal agencies provides comparative information for the Coast Guard's planning. With the vast number of threats and actors in the maritime domain, the Coast Guard has focused a great deal on training and staying ahead of the problem to defend cyberspace.[169]

2. Enabling Operations

The two goals of enabling operations are to "incorporate cyberspace operations into mission planning and execution, and [to] deliver cyber capabilities to enhance all

---

167 "United States Coast Guard Cyber Strategy." Washington, DC. June 2015, 24–5, https://www.U.S.C.G.mil/seniorleadership/DOCS/cyber.pdf.

168 Maureen D. Johnson, "Department of Homeland Security Efforts: Implementing Cybersecurity Initiatives Throughout the Federal Government." *Coast Guard Proceedings*, vol. 71, no. 4 (2014–2015):53. http://uscgproceedings.epubxp.com/i/436751-win-2015.

169 "United States Coast Guard Cyber Strategy." Washington, DC. June 2015, 23–5, https://www.U.S.C.G.mil/seniorleadership/DOCS/cyber.pdf.

missions."[170] The Coast Guard's unique role as both an intelligence asset and a law enforcement agency create unique opportunities to protect the maritime cyber realm. According to the Coast Guard's 2015 *Cyber Strategy*, "The Coast Guard will leverage approaches, processes, tools, and authorities that will maximize our effectiveness amongst—and against—diverse and sophisticated adversaries in the cyber domain"[171]

While maintaining a resilient cyber domain for maritime operations in the United States, the Coast Guard enables its commanders the capabilities and assets necessary for maritime cybersecurity. One of the most crucial assets the Coast Guard has at its disposable is cyberspace operation personnel who are specifically trained for cyber missions. These personnel are recruited and trained to "create a professional cadre with specialized skills in cybersecurity, cyber intelligence, cyber law enforcement missions, cyber support to critical infrastructure, and cyber … operations."[172] Specialists in the field are responsible for safety, security, and cyber resilience of the MTS.

3. Protecting Infrastructure

The MTS has critical infrastructure in the United States that requires security systems throughout in order to maintain the security and prosperity of the American maritime system. The Coast Guard accepts the burden of protecting the maritime infrastructure and the MTS during cyber threats, natural disasters, and kinetic attacks. The two goals of protecting infrastructure include "risk assessment—promote cyber risk awareness and management, and prevention—reduce cybersecurity vulnerabilities in the MTS."[173] The Coast Guard's main efforts reside in the relationships it establishes with civilian components working together to prevent cyber threats.

---

170 "United States Coast Guard Cyber Strategy." Washington, DC. June 2015, 27–9, https://www.U.S.C.G.mil/seniorleadership/DOCS/cyber.pdf.

171 Ibid, 27.

172 Ibid, 28.

173 Ibid, 31–2.

4. Summary

The Coast Guard is responsible for overall maritime cybersecurity in the United States. Balancing both military operations and civilian-side cybersecurity, the Coast Guard has an enormous responsibility toward national security and the cyber realm. Because the task is so great, outside federal and civilian agencies must work together with the Coast Guard to maintain cyber resilience.

B. SUPPORTING AUTHORITIES OF MARITIME CYBERSECURITY

The lead agency responsible for maritime cyber security within the United States is the DHS through the USCG. The Coast Guard cannot do the job alone and relies on outside partnerships that it develops among sister agencies in the U.S. government. These partnerships are crucial for maintaining order in all aspects of the maritime community. Furthermore, groups, such as the Homeland Infrastructure Threat and Risk Analysis Center, the United States Computer Emergency Readiness Team, the Industrial Control Systems Cyber Emergency Response Team, and the National Infrastructure Coordination Center, are all on standby to support the maritime domain in the United States with any means necessary.[174] These agencies work through parent departments in DHS, not only in times crisis but also for prevention.

1. Federal Bureau of Investigation and Cybersecurity

Along with giving the Coast Guard authority to uphold cybersecurity in the maritime domain, PPD 21 grants privileges to the FBI to maintain cyber resilience throughout the United States. In 2003, the FBI created its cyber division and placed cyber warfare as the FBI's number three national priority, behind counterterrorism and counterintelligence.[175] The FBI specifically "collects, analyzes, and disseminates domestic cyber threat information to interagency partners and the private sector."[176] According to the FBI, billions of dollars are lost annually because cyber threats target

---

[174] Johnson, "Department of Homeland Security Efforts," 53.

[175] Kolko, "Countering the Maritime Cyber Threat," 60.

[176] Ibid.

crucial infrastructure and systems on which many rely. To fully embrace the cyber threat, the FBI has created different programs and partnerships with law enforcement agencies across the United States, including a cyber division at FBI headquarters, cyber squads working out of 56 different field offices, cyber action teams deployable anywhere in the United States, computer crimes task forces working with state and local authorities on cybercrimes, as well as DOD and DHS support.[177]

a. The FBI and Coast Guard Relationship

Conducting exercises builds the foundation on which a maritime cyber threat can be defeated. FBI and Coast Guard authorities participate in joint exercises throughout the year to better their efforts against cyber threats, build teamwork and unity, and train with the latest techniques. Better insight into one such exercise is provided by Supervisory Special Agent Richard Kolko of the FBI's Cyber Division. Kolko outlines an actual drill in which Coast Guard and FBI agents disrupt a cyber-attack:

> A team of FBI agents from the cyber task force and Coast Guard Investigative Service meet in a warehouse on the outskirts of a major port on the West Coast to review the operations plan for a search warrant to be served on a nearby shipping office. The warrant is based on a cybercriminal intrusion into the office's computer system. The goal of the criminals in this scenario is to affect delivery of food shipments into the busiest port in the U.S. by hacking into the company's network, which can impact citizens through even a slight delivery delay.[178]

The FBI–Coast Guard partnership is critical for supporting maritime cyber operations and preventing attacks. Cyber Division's Assistant Director Joseph Demarest explains that the exercise simulates the FBI's and Coast Guard's official response, which triggers collaborative responses at all levels of government.[179]

---

177 Federal Bureau of Investigation, "National Cyber Investigative Joint Task Force." Last accessed April 15, 2016. https://www.fbi.gov/about-us/investigate/cyber/ncijtf.

178 Kolko, "Countering the Maritime Cyber Threat," 58.

179 Kolko, "Countering the Maritime Cyber Threat," 59.

b. National Cyber Investigative Joint Task Force

Established by the FBI in 2008, the National Cyber Investigative Joint Task Force (NCIJTF) consists of more than 20 government agencies responsible for coordinating and integrating cyber-threat investigation services for national security.[180] Figure 3 depicts the members of NCIJTF.

Figure 2. NCIJTF Members[181]

What makes NCIJTF function is the ability of federal, state, and local authorities to work in unison. This union allows members to access the most up-to-date listing of cyber threats available through intelligence gathering and collaboration. Greg McAleer, a Secret Service agent in charge of cyber security states, "The NCIJTF uses a whole government approach—employing every tool in our arsenal to address the threat and

180 Federal Bureau of Investigation. "National Cyber Investigative Joint Task Force." Last accessed April 15, 2016. https://www.fbi.gov/about-us/investigate/cyber/ncijtf.

181 Source; Kolko, "Countering the Maritime Cyber Threat," 59.

protect our infrastructure, financial systems, and intellectual property."[182] Success in national cybersecurity means joint cooperation. Joint cooperation includes outside agencies providing data for the maritime community. Although agencies in NCIJTF are focused on maintaining a cyber-resilient United States, the attention and efforts of these agencies may not always be focused specifically on maritime cybersecurity. Although this alliance and cooperation exists among federal agencies, it does not relieve the Coast Guard of its primary role and focus on the maritime realm.

2. Critical Infrastructure Cyber Community

As a direct result of Executive Order (EO) 13636, the DHS established a voluntary cyber community, creating opportunities for public and private owners of critical infrastructure in the United States. The program, known as C-Cubed, establishes a forum for its members that provides guidance and resources to address cyber risks. The program influences members of the public and private sector who seek out assistance from the DHS in direct support of cyber threats. C-Cubed "support[s] industry to increase cyber resilience, promote[s] cybersecurity framework awareness, [and] encourage[s] organizations to manage cybersecurity as part of an all-hazards approach to enterprise risk management."[183]

The focus of the program is on all aspects of cybersecurity in the United States, not just maritime cybersecurity. Companies providing water and energy or those responsible for maintaining air travel, for example, participate in the C-Cubed program to minimize risks. The program works as a one-size-fits-all approach for infrastructure in the United States in an effort to maintain an overall cyber-resilient nation.[184]

---

[182] Federal Bureau of Investigation, "Cyber Security: Task Force Takes 'Whole Government' Approach." October 20, 2014. https://www.fbi.gov/news/stories/2014/october/cyber-security-task-force-takes-whole-government-approach.

[183] Thad Odderstol, "C-Cubed: Increasing cyber resilience, awareness, and managing risk." *Coast Guard Proceedings* 71, no. 4 (2014–2015): 12–3. http://uscgproceedings.epubxp.com/i/436751-win-2015.

[184] Odderstol, "C-Cubed," 14.

3. Summary

Although there are outside entities that support the Coast Guard, particularly the FBI, the Coast Guard is still responsible for the overall maritime domain in the United States. The establishment of the NCIJTF as a cybersecurity forum is good for basic cyber support and strategy. Unfortunately, many of the federal agencies that make up NCIJTF have nothing to do with the maritime industry and, therefore, provide no benefit to maritime cyber resilience. If a massive coordinated cyber-attack on the United States were to take place, it is unclear where the maritime industry would fall on the priority list for restoring capabilities. While it is good practice to form interagency relationships, the Coast Guard should not rely solely on the FBI or members of the NCIJTF in an era that stresses national security.

C. THE EUROPEAN UNION AND CYBERSECURITY

Joint cybersecurity efforts in the EU began in 2001, when the EU Commission implemented the Network and Information Security (NIS) policy. In 2006, the EU Commission released the Strategy for a Secure Information Society and in 2009, the Critical Information Infrastructure Protection (CIIP) plan. These laws established the framework the EU upholds today.[185]

Member states in the EU ultimately own responsibility for protecting individual network systems. ENISA, Europol, and the European Defense Agency (EDA) are the three main organizations responsible for coordinating cyber efforts for all the member states in the EU. ENISA responsibilities fall within network and information security, Europol focuses on the law enforcement aspect, and the EDA coordinates joint cyber defenses for the EU. With support from organizations at the national level, the EU

185 European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace." Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions. July 2, 2013. 5. https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-Internet-and-online-freedom-and-opportunity-cyber-security.

provides the most favorable responses, deterrence, and strategies possible.[186] Figure 4 depicts the hierarchy of the EU's cyber strategy.[187]

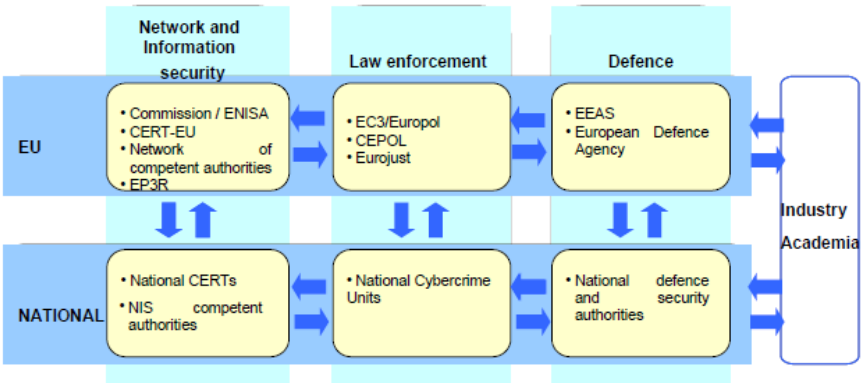

Figure 3. European Commission: The EU's Cybersecurity Roles and Involvement[188]

1. Cybersecurity Strategy of the European Union

The Cybersecurity Strategy of the European Union was signed into law on July 2, 2013, providing guidance for short- and long-term strategies for the EU. The six strategies adopted by the EU are as follows:

> achieving cyber resilience; drastically reducing cybercrime; developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP); develop[ing] the industrial and technological resources for cybersecurity; establish[ing] a coherent international cyberspace policy for the European Union[;] and promot[ing] core EU values.[189]

---

[186] European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace." Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions. July 2, 2013. 17. https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-Internet-and-online-freedom-and-opportunity-cyber-security.

[187] Ibid.

[188] Source: Ibid.

[189] European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace." Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions. July 2, 2013. 4–5. https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-Internet-and-online-freedom-and-opportunity-cyber-security.

The EU Committee understands the looming threats of cyber-attacks in the EU or in member states. These six strategies of the EU established a framework for national and state governments to manage their own cybersecurity responsibilities for themselves and the greater EU.

First, achieving cyber resilience to the EU means the private and public sectors work together during the preparation phases and, if necessary, the response phases. To ensure the goal of cyber resilience is being met, the EU cybersecurity strategy requires computer emergency response teams (CERTs-EU) to coordinate prevention as well as support the private sector, which has little incentives or monetary allowances from the EU to develop or expand its cyber resilience. One of the first directives from the EU Committee is for ENISA to establish a voluntary certification program for IT specialists to determine the effectiveness of training and abilities of employees. Other priorities consist of creating cyber awareness month, organizing school training sessions, and inviting academics from member states to provide solutions for cyber problems. Awareness among the member states is vital in a cyber-resilient EU.[190]

Second, the EU's economy suffers from cyber-attacks and criminal activity.[191] In order to reduce cybercrime in the EU, member states have ratified the Council of Europe Convention on Cybercrime, an agreement that outlines rules and regulations for national cybersecurity crimes. This legislation mandates that a member state develop a cybercrime law-enforcement agency within its borders to defend and track down internal cyber criminals. The EU provides the funding for the member state to establish and maintain appropriate law enforcement agencies. The European Cybercrime Centre (EC3), a part of Europol, directs member states in best practices for reducing cybercrime.[192]

Third, the EU recognizes cyber threats involve military, civilian, and government authorities working together to develop a responsive cyber-defense policy with corresponding capabilities. The EU recognizes the potential to work with members of the

---

[190] Ibid, 5–8..

[191] Ibid, 3.

[192] European Commission, “Cybersecurity Strategy,” 9–10.

North American Treaty Organization (NATO), to which a majority of the EU belongs. However, the strategy does not list what is an appropriate retaliatory measure based on a cyber-attack. The strategy provides little guidance as the information regarding EU cyber-defense strategies is most likely classified.[193]

Fourth, the EU believes private-sector industry partners that develop technology for the cyber sector must be willing to make security a top priority for their own technologies to maintain resiliency in the EU. In order to ensure the private sector complies with the wishes of the EU Commission, incentives must be given to the private sector for demanding such security devices are standardized across the board.[194] The Commission directs ENISA as well as investors in the public and private sectors to develop strategies and programs that are in line with the Commission's purpose.

Finally, the Commission recognizes that although the EU has moved toward developing a more resilient cyber domain, without the support of the international community—including other nations, private industry representatives, and the public sector—the cyber domain will never be fully resilient. Specifically, relations with the UN and NATO, for example, will provide access to an international stage that enables proponents of multinational cyber-realm abilities to address issues.[195] Recognizing the necessity for the international community to work together is critical for national security interests, not only in the EU but also in the United States.

2. European Union Maritime Security Strategy

The EU ratified the European Union Maritime Security Strategy (EUMSS) in 2014 as the primary framework for maritime security. Realizing that the maritime industry is an absolute necessity to the EU, member states united to ensure EU fleets, critical infrastructure, and the markets remain resilient. The EUMSS recognizes nine major threats to maritime security in the EU, including cyber-attacks. Although this

---

[193] Ibid, 11–13.

[194] Ibid, 12–13.

[195] Ibid, 14–17.

particular legislation covers a variety of threats, the legislation establishes five areas in which member states work together to remain resilient.[196]

The five concentrations of EUMSS include external action; maritime awareness, surveillance, and information-sharing; capability development; risk management, protection of critical infrastructure, and crisis response; and maritime security research and innovation, education, and training.[197] EUMSS goals are similar to those of the maritime cyber strategy of the EU; however, the EUMSS specifically focuses on the threats associated with the maritime domain. Each specific focus explains how member states will achieve sector-specific goals. The conclusion of EUMSS states,

> The Council, Member States, Commission and High Representative have developed this Strategy in a joined-up manner. This has been an efficient way of working that should continue, including all relevant stakeholders and actors both at EU and national level.[198]

The main takeaway from the EUMSS is the ability for the member states to come together as one and agree on a strategy that benefits the EU as a whole, thus making the EU more resilient to maritime threats. The collective defense of the EU, through international rules and laws including UNCLOS and various legislations, creates a better positioned EU.

D. REPORTING A MARITIME CYBER-ATTACK

While working to establish governance and solutions for tomorrow's attacks today, the United States and the European Union have defined responsibilities and legislation to deal with potential threats. Although responsibilities are outlined, the authority to respond to such attacks seems unclear. The Coast Guard in the United States and Europol in the EU are the two agencies responsible for law enforcement in maritime cybersecurity. To determine whether these agencies could respond to a cyber-attack at a

196 General Secretariat of the Council, "European Union Maritime Security Strategy." June 24, 2014.8. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT.

197 Ibid, 8–14.

198 Ibid, 15.

moment's notice, it is necessary to evaluate the reporting criteria of a cyber-attack. The following portion of this section presents a scenario in which the United States and Great Britain respond to a non–U.S. flagged commercial vessel and a non–EU flagged commercial vessel, respectively, at a distance of 14 nautical miles from shore. The captain has lost control of the engine, steering, and navigational equipment aboard his vessel, similar to the research conducted at the University of Texas. The vessel is a liquid natural gas (LNG) tanker traveling at best speed and cannot stop. Who does the captain call?

The Coast Guard has no formal check sheet or pre-planned response for masters of vessels who find their systems hacked and unresponsive. Despite the efforts and legislation established in Washington, a master of a vessel would be left to deal with the situation using one of the following options: dropping anchor to stop the ship's movement provided he has sufficient depth or manually overriding the ship's sensors and IT system through mechanical means. Europol, like the Coast Guard, does not have an immediate response check sheet for mariners who find themselves under a cyber-attack on the open ocean, which leaves masters helpless.

However, CERT-EU and the FBI have official online forms that members of the maritime community can submit to report a cyber-attack or phishing incident.[199] These online forms allow users to complete an incident response that moves its way through the proper channels. Europol has its own dedicated website for cybercrimes in member states. However, the reporting criteria for each country are different. For example, when clicking on the link for Austria, the victim of a cyber-attack is directed to an email address without specific questions. When accessing the page for Germany, the link guides victims to a series of phone numbers to contact cyber specialists in Germany.[200] The real question is if a cyber-attack is taking place on a ship, how is the ships company

199 "Report Cyber Incidents." Department of Homeland Security. Last accessed April 26, 2016. https://www.dhs.gov/how-do-i/report-cyber-incidents.

200 "Report Cybercrime." Europol. Last accessed April 26, 2016. https://www.europol.europa.eu/content/report-cybercrime.

able to make an online report of a cyber-attack, assuming the ships network is compromised? Despite the push for a joint cyber strategy from the EU, member states have significantly different reporting criteria, and none have responses specifically for the maritime industry.

E. SUMMARY

Maritime cybersecurity and, thus, national security for the United States begins within the borders of the 50 states as well as within other nations around the world. Defeating and deterring maritime cyber-attacks in the United States require a joint comprehensive strategy, agreed upon by all members of the maritime community. The Coast Guard is primarily responsible for maritime cybersecurity, but evidence shows the Coast Guard would be limited in dealing with a call on a VHF radio from a master at sea who is under attack. The players involved in cybersecurity in the United States are countable, thus giving responsibility to everyone and fuzzy authority to no one in particular. Although the EU's collective security seems ideal, some member states still doubt the seriousness of a cyber threat or appear ignorant of such events, as mentioned in Chapter III. To date, no formal process or protocol has been established to provide mariners guidance for resolving a cyber-attack at sea.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS

> The guardians of your company's cybersecurity should be encouraged to network within the industry to swap information on the latest hacker tricks and most effective defenses.
>
> —Nina Easton[201]

The cyber realm for the maritime community is an iceberg waiting to hit the *Titanic*. Without proper foresight—and the ability for leaders in the maritime community to come to terms with their glaring cybersecurity vulnerabilities—it will only be a matter of time until a maritime cyber-attack affects national security in the United States. Although research has been conducted and different entities have identified threats to the maritime community, the examination revealed that cyber resilience in the United States has been taken lightly.

This chapter evaluates the studies on maritime cybersecurity, in particular, focusing on the lack of cyber awareness and training within the community, the equipment vulnerabilities, and governance already in place. Next, it provides policy recommendations for both the United States and the international community to develop a conversation on a global maritime cyber strategy. Finally, it suggests areas for future research.

A. EVALUATION OF THE MARITIME CYBER THREAT

No two cyber-attacks are alike. When dealing with a vast domain of networks, systems, and equipment, criminals have their pick of vulnerable networks to infiltrate. It is the job of the private and public sectors in the United States to ensure the nation's waterways remain open.

---

201 *Brainy Quote* s.v. "Quotes by Nina Easton," accessed April 26, 2016, http://www.brainyquote.com/quotes/quotes/n/ninaeaston720079.html.

1. Lack of Cyber Awareness and Training in the Community

It is one thing for experts in the field of cybersecurity to understand the problem of cyber threats; it is another thing entirely to convince and educate operators at every level of the urgency to prepare for them. Both Kramek's report and ENISA's findings suggest that maritime cyber security was insufficient and in some cases, "nonexistent."[202] The lack of understanding within the international community is concerning for experts who stress the importance of maritime cybersecurity. ENISA recommends cyber awareness trainings and campaigns that focus on all members in the maritime domain, including stevedores, terminal operators, and sailors, to broaden the understanding of the maritime community.[203] The trainings and certifications can be conducted throughout the year as necessary by supporting government authorities that regulate and standardize the process. Informing all maritime members of the challenges in cybersecurity could provide a first line of defense to prevent accidental cyber incidents by employees, as explained in Chapter III.

2. Equipment Vulnerabilities and Backup Procedures

The maritime community's reliance on technology will continue to expand in the future. Technology is a boon for operators across different platforms who want to maximize efficiency and work output. Despite its benefits, technology has become a crutch for many members in the maritime community. In order to maintain equipment resiliency, the civilian maritime community must continue to teach celestial navigation, which relies on observing the position of stars rather than on using GPS to confirm a vessel's position."[204] The Merchant Marine Academy, located in Kings Point, New York, still teaches celestial navigation for its prospective third mates; and, the Naval Academy has begun to offer celestial navigation again as part of its curriculum after a ten-year

---

[202] "Analysis of Cyber Security Aspects," ENISA, 1.

[203] Ibid.

[204] Dictionary.com, "Celestial navigation." Last accessed May 9, 2016. http://www.dictionary.com/browse/celestial-navigation.

hiatus.[205] Top officials at the Naval Academy understand that today, with the developing cyber threats in the maritime domain, that backup procedures like celestial navigation are crucial to resiliency.

Radiofrequency navigation is no longer used in the United States. Developed during WWII, the long-range navigation (LORAN) system was an aid that used low frequency radio signals from a land base to help mariners determine their position at sea. The Coast Guard operated LORAN throughout the coastal waters of the United States until February 8, 2010. According to the Navigation Center of the Coast Guard, "as a result of technological advancements in the last 20 years, [LORAN] became an antiquated system no longer required by the armed forces, the transportation sector or the nation's security interests."[206] Although LORAN no longer transmits signals out to sea, the Coast Guard should consider keeping LORAN stations operational with limited funding in case a cyber-attack renders GPS or other electronic aids to navigation useless. With the infrastructure already in place for these systems, a cost–benefit analysis of keeping the towers operational should be conducted.

Manual backup procedures of networks must happen to ensure proper inventory control. The ability for a terminal to have hard copies of its inventory could provide shipping and receiving accurate information in case a cyber-attack takes place at the facility. CyberKeel states,

> Cyber resilience would include clear plans for alternate communication channels, alternate informational databases fully independent from daily systems as well as alternate tools and systems onboard vessels to ensure operations if normal systems are breached or jammed.[207]

---

[205] Andrea Peterson, "Why Naval Academy students are learning to sail by the stars for the first time in a decade." The Washington Post. February 17, 2016. https://www.washingtonpost.com/news/the-switch/wp/2016/02/17/why-naval-academy-students-are-learning-to-sail-by-the-stars-for-the-first-time-in-a-decade/.

[206] Navigation Center, "Loran-C General Information." U.S. Department of Homeland Security United States Coast Guard. Last accessed May 9, 2016. http://www.navcen.uscg.gov/?pageName=loranMain.

[207] CyberKeel, "Maritime Cyber-Risks," 24.

As seen from the example of the Islamic Republic of Iran Shipping Lines (IRISL), in which the complete inventory on hand was completely lost, the ability to have printed copies of inventory will cost very little but yield a larger return if needed. Cyber resiliency in the maritime community is almost prepared to maintain normal operations and limit cyber threats.

3. Maritime Cybersecurity Governance in the United States

The United States and the EU both have general legislation in place that establishes certain guidelines for the maritime communities inside their borders. The United States has given authority and responsibility to the USCG for cybersecurity incidents, and the EU has given ENISA, EUROPOL, and the EDA different responsibilities for ensuring cyber resilience within the EU's borders. However, both the United States and the EU lack a common approach and do not have a standard for cybersecurity regulation. The lack of regulation in the EU and in the United States is a cause for concern over how secure U.S. ports are from cyber-attacks.

The Coast Guard has the support of the NCIJTF in matters of cybersecurity; however, one needs to question how responsive or useful NASA, for example, would be toward maritime cybersecurity or where maritime cybersecurity falls within the grand scheme of a multi-infrastructure cyber-attack in the United States. The complexity of the NCIJTF with 19 different players involved seems to be inappropriate for maritime cybersecurity. The United States should acknowledge network and information security, law enforcement, and defense in the maritime cyber community as three different entities reporting to one superior in order to maximize capabilities and resiliency.

B. POLICY RECOMMENDATIONS FOR THE MARITIME COMMUNITY

Although many issues have come to light in the research of maritime cybersecurity, experts in the field offer solutions for how to establish and maintain a resilient cyber infrastructure for the maritime community. In order for these recommendations to benefit the national security of the United States, the U.S. government as well as private and public sectors involved in the maritime community

must agree that the United States has a maritime cyber problem, which must be resolved before disaster strikes.

One of the biggest critics of maritime cybersecurity in the United States is Kramek. Based on his criticisms, Kramek makes useful policy recommendations for Congress, DHS, and PSGM administrators; the Coast Guard; and terminal owners, operators, and their respective security officers. First, Kramek recommends that Congress conduct its own study and set forth requirements for the Coast Guard through specific legislation that grants authority to establish an inspection team. Second, Kramek recommends that DHS and PSGM administrators dedicate funding based on the cyber threats listed in this thesis to strengthen cybersecurity in the United States. Third, Kramek recommends the Coast Guard engage all sectors of the maritime community, including the IMO, in a global campaign to raise awareness and to enforce cybersecurity standards. Finally, Kramek recommends that terminal owners, operators, and their respective security officers conduct vulnerability assessments, establish preplanned responses for their specific cybersecurity needs, and request additional funding for implementing cybersecurity requirements.[208]

ENISA's analysis concludes with goals for the EU and is broken up into short-, mid-, and long-term priorities. First, short-term priority recommendations encourage discussions among members of the maritime community in the EU on maritime cyber issues in an attempt to raise awareness and develop best practices. Second, mid-term policy priorities recommend that cybersecurity trainings are conducted throughout the maritime industry and that the EU develop specific roles for member states, so they participate in the joint efforts of EU cybersecurity. These roles and other rules affecting EU cybersecurity postures would be established in new legislation agreed upon by the EU maritime community. Finally, ENISA recommends that the EU enforce the regulations established by the maritime community and work toward an international approach for a unified cyber strategy that all signatory nations would abide by.[209]

---

[208] Kramek, "The Critical Infrastructure Gap," 33.

[209] "Analysis of Cyber Security Aspects," ENISA, 20.

Throughout CyberKeel's white paper, recommendations for policy changes consistently appear. One of the major concerns experts at CyberKeel noted was the overall lack of honesty in reporting cyber-attacks on the global maritime community.[210] The maritime community must be open about cyber-attacks within their areas for two main reasons. First, once the community is aware an attack has taken place, other terminals, vessels, or ports can work to strengthen their defenses against similar attacks. Second, when a member of the maritime community reports a cyber-attack after it takes place, instead of keeping the information of the attack private, it should seek out advice from security firms across the United States—whose sole purpose is to develop lessons and procedures for restoring systems or deterring attacks in the first place. Because ports of different tiers in the United States receive different amounts of funding, the ability for a small port to access lessons learned from a larger port may come in useful when fighting off potential cyber-threats. CyberKeel is developing a forum to establish trust and openness among members to unite the maritime industry toward cybersecurity best practices.[211]

Others have come forward stating that the maritime community must take action, focus resources, and develop strategies for securing the maritime cyber community. In March 2016, the Office of Cyber and Infrastructure Analysis (OCIA) made many similar recommendations to those of Kramek, ENISA, and CyberKeel many years earlier. Some of OCIA's recommendations include cyber strategies, vulnerability assessments, workplace trainings that cover the threats of phishing scams and the need for frequent password updates, as well as manual electronic data backup.[212] That the same recommendations have been made before validates the seriousness of the maritime cyber realm.

---

[210] "Maritime Cyber-Risks," CyberKeel, 4.

[211] Ibid, 25.

[212] "Consequences to Seaport Operations," OCIA, 17.

National security and cybersecurity in the United States must take a universal approach through the IMO as recommended previously by ENISA. Assuming the United States takes a progressive step toward awareness, vulnerability assessments, and cybersecurity funding, the nation will always be at risk for a maritime cyber-attack if the international community cannot enforce a global standard. Global maritime governance is ultimately required for the maritime cybersecurity of each nation.

C. AREAS FOR FURTHER RESEARCH

This thesis serves as the cornerstone for recommendations among the maritime community and governing bodies in the United States. With the limited information available on U.S. maritime cybersecurity, this thesis evaluated U.S. policies and ports against those of the European Union. Another possible approach toward evaluating cybersecurity in other nations around the world is through a standardized assessment conducted by an international organization, preferably, the IMO. Success in maritime cybersecurity and, thus, national security extends beyond the territorial waters of the United States. In order to achieve success, the international community, including decision makers in Washington, must agree upon international governance, protocols, and legislation. While this thesis compared top-tier ports in the United States and evaluated each port's ability to respond to cyber threats, the same kind of data was not available for EU port facilities. The ability for a standardized evaluation will address the same concerns on an even playing field across all maritime nations. These standardized checklists can be used to evaluate a port's status at any time for both self-assessment purposes and for more formal inspections.

Further comparisons should be made between maritime nations in the European Union. Although this thesis applies broad information regarding maritime cybersecurity to the United States and the EU as a whole, research should be conducted for nations outside this sample to further evaluate how maritime nations address cybersecurity. If other maritime nations have stronger maritime cyber strategies than those of the United States or EU, the strategies should be evaluated in a U.S. policy directive to serve the national security interests of Washington.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Bateman, Tom. “Police Warning after Drug Traffickers’ Cyber-attack.” *BBC News*, Oct 16, 2013. http://www.bbc.com/news/world-europe-24539417.

Belmont, Kate B. “Maritime Cyber Attacks: Changing Tides.” Blank Rome Counselors at Law. November 16, 2015. https://www.blankrome.com/index.cfm?contentID=37&itemID=3734.

Bender, Dan. “How the Sinking of the Titanic Changed the World.” *Coast Guard Compass*, Official Blog of the U.S. Coast Guard. April 14, 2010. http://coastguard.dodlive.mil/2010/04/how-the-sinking-of-the-titanic-changed-the-world/.

Bensalhia, John. “Cyber-attacks on U.S. Ports Risk Chemical Disaster.” The Stack. Oct 12, 2015. https://thestack.com/security/2015/10/12/cyber-attacks-on-u-s-ports-risk-chemical-disaster/.

Bivens, Danielle. “Maritime Governance: Designed with Security in Mind.” *Coast Guard Proceedings* 71, no. 4 (2014–2015): 6-7. http://uscgproceedings.epubxp.com/i/436751-win-2015.

Colvin, Geoff. "Adm. Mike Mullen: Debt Is Still Biggest Threat to U.S. Security." *Fortune*, May 10, 2012. http://fortune.com/2012/05/10/adm-mike-mullen-debt-is-still-biggest-threat-to-u-s-security/.

Commandant of the Coast Guard. “Cyber Security and the Marine Transportation System.” Message Traffic. August 2, 2013. http://www.uscg.mil/announcements/alcoast/323-13_alcoast2.txt.

Council of the European Union, "European Union Maritime Security Strategy," June 24, 2014, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT.

CyberKeel, “Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas,” October 15, 2015, http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf.

Department of Homeland Security, “National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security,” October 2005, https://www.dhs.gov/sites/default/files/publications/HSPD_MDAPlan_0.pdf.

———. “Report Cyber Incidents,” March 4, 2016, https://www.dhs.gov/how-do-i/report-cyber-incidents.

Dodge, Edward. “How Dangerous is LNG?” *Breaking Energy*, October 22, 2014. http://breakingenergy.com/2014/12/22/how-dangerous-is-lng/.

Donati, Jessica, and Daniel Fineren, “Exclusive: Iran Shipping Signals Conceal Syria Ship Movements.” *Reuters*, Dec 6, 2012. http://www.reuters.com/article/us-syria-iran-tracking-idUSBRE8B50KX20121206.

eModal. “eModal.” Accessed March 22, 2016. http://welcome.emodal.com/.

European Network and Information Security Agency (ENISA), “Analysis of Cyber Security Aspects in the Maritime Sector,” November 2011, https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/dependencies-of-maritime-transport-to-icts.

European Commission, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,” July 2, 2013, https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-Internet-and-online-freedom-and-opportunity-cyber-security.

European Union, “The EU Maritime Security Strategy and Action Plan: Information Toolkit,” accessed April 20, 2016, http://eeas.europa.eu/maritime_security/docs/maritime-security-information-toolkit_en.pdf.

Europol. “Report Cybercrime.” Accessed April 26, 2016. https://www.europol.europa.eu/content/report-cybercrime.

Federal Bureau of Investigation (FBI). “Cyber Security: Task Force Takes ‘Whole Government’ Approach,” October 20, 2014, https://www.fbi.gov/news/stories/2014/october/cyber-security-task-force-takes-whole-government-approach.

———. “National Cyber Investigative Joint Task Force.” Accessed April 15, 2016. https://www.fbi.gov/about-us/investigate/cyber/ncijtf.

Federal Emergency Management Agency (FEMA). “FY 2012 Port Security Grant Program (PSGP).” Accessed March 26, 2016. https://www.fema.gov/fy-2012-port-security-grant-program.

———. “Fiscal Year (FY) 2016 Port Security Grant Program (PSGP) Notice of Funding Opportunity (NOFO). Accessed March 26, 2016. https://www.fema.gov/media-library/assets/documents/114444.

Fellman, Sam. “VCNO Michelle Howard Pushes for Cyber Vigilance, More Women in the Ranks.” *Navy Times*, April 12, 2015. http://www.navytimes.com/story/military/pentagon/2015/04/12/vcno-michelle-howard-cyber-vigilance-more-women-navy-ranks/70774264/.

Ferran, Lee. “The Guys Who Can Make Oil Tankers Disappear, Virtually.” *ABC News*, Oct 15, 2013. http://abcnews.go.com/Blotter/guys-make-oil-tankers-disappear-virtually/story?id=20565851.

Fisher, Leigh. "Strategic Plan Presentation Prepared for the Port of Houston Authority," April 28, 2015, http://www.portofhouston.com/static/gen/inside-the-port/Strategic%20Planning/PHA_Strategic_Plan_Approved_2015-0428_(FINAL).pdf.

Gertz, Bill. “Iran Rapidly Building Cyber Warfare Capabilities.” *The Washington Free Beacon*, May 12, 2015. http://freebeacon.com/national-security/iran-rapidly-building-cyber-warfare-capabilities/.

Goreman, Steve. “U.S. West Coast Ports Closed to Cargo Vessels Again for Weekend.” *Reuters*, February 13, 2015. http://www.reuters.com/article/us-usa-ports-west-idUSKBN0LH2CK20150214.

History. "This Day in History: April 15." Accessed February 4, 2016. http://www.history.com/this-day-in-history/titanic-sinks.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). “Cyber Threat Source Descriptions.” Accessed April 3, 2016. https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions#nat.

Jensen, Lars. “Challenges in Maritime Cyber-Resilience.” *Technology Innovation Management Review* 5, no. 4 (April 2015): 35-8. http://timreview.ca/article/889.

Johnson, Maureen D. “Department of Homeland Security Efforts: Implementing Cybersecurity Initiatives throughout the Federal Government.” *Coast Guard Proceedings* 71, no. 4 (2014–2015): 53. http://uscgproceedings.epubxp.com/i/436751-win-2015.

Karr, Clinton. “Mitigate Insider Threats With a Measured Approach to Security.” *Reuters*, Oct 24, 2012. http://www.reuters.com/article/idUS146971+24-Oct-2012+HUG20121024.

Kaspersky Lab, “The ‘Icefog’ Apt: A Tale of Cloak and Three Daggers.” 2013. http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/icefog.pdf.

———. “Kaspersky Lab exposes ‘Icefog’: a New Cyber-Espionage Campaign Focusing on Supply Chain Attacks.” September 26, 2013. http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_exposes_Icefog_a_new_cyber-espionage_campaign_focusing_on_supply_chain_attacks.

Kolko, Richard. “Countering the Maritime Cyber Threat.” *Coast Guard Proceedings* 71, no. 56. (2014–2015): 55-61. http://uscgproceedings.epubxp.com/i/436751-win-2015.

Kramek, Joseph. “The Critical Infrastructure Gap: US Port Facilities and Cyber Vulnerabilities.” Brookings. July 3, 2013. http://www.brookings.edu/research/papers/2013/07/03-cyber-ports-security-kramek.

Lennon, Mike. “‘Icefog’ Cyber Attacks Targeted U.S. Energy Firms Using Java Backdoor.” *Security Week*, January 14, 2014. http://www.securityweek.com/icefog-cyber-attacks-targeted-us-energy-firms-using-java-backdoor.

———. “Attacks Against SCADA Systems Doubled in 2014: Dell. *Security Week*, April 13, 2015. http://www.securityweek.com/attacks-against-scada-systems-doubled-2014-dell;%20A.

Maritime Executive, “10 Years After 9/11, Security Still a Top Priority for U.S. Ports,” September 2, 2011. http://www.maritime-executive.com/article/10-years-after-9-11-security-still-a-top-priority-of-u-s-ports.

———. “Iran’s Offshore Platforms Become Target to Recent Cyber Attacks,” October 9, 2012. http://maritime-executive.com/article/iran-s-offshore-platforms-become-target-of-recent-cyber-attacks.

Maryland Port Administration, “Strategic Plan 2015,” September 2015, http://www.mpa.maryland.gov/_media/client/planning/Strategic__Plan%202015.pdf.

Menn, Joseph, and Warren Strobel, “New NSA Chief Vows More Transparency for Embattled Agency.” *Reuters*, May 12, 2014. http://www.reuters.com/article/us-cyber-summit-nsa-rogers-idUSBREA4B0XU20140512.

Middleton, Allison. “Hide and Seek: Managing Automatic Identification System Vulnerabilities.” *Coast Guard Proceedings* 71, no. 4 (2014–2015): 48-9. http://uscgproceedings.epubxp.com/i/436751-win-2015.

Mohammed, Arshad, Matt Spetalnick, and Mark Hosenball. “Exclusive: U.S. Weighs Sanction Russia as well as China in Cyber Attacks.” *Reuters*, September 1, 2015. http://www.reuters.com/article/2015/09/01/us-usa-cybersecurity-russia-exclusive-idUSKCN0R12FE20150901#0wKGvOQlmoE6SXDF.97.

Mueller, Robert S., III. “Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies." Speech for the RSA Cybersecurity Conference, San Francisco, CA, March 1, 2012. https://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

NAVIS. “About NAVIS N4.” Accessed, March 26, 2016. http://navis.com/get-more-n4.

Newberry, Marshall, E. “Maritime Critical Infrastructure Cyber Risk.” *Coast Guard Proceedings* 71, no. 4 (2014–2015): 42-44. http://uscgproceedings.epubxp.com/i/436751-win-2015.

Odderstol, Thad. “C-Cubed: Increasing Cyber Resilience, Awareness, and Managing Risk.” *Coast Guard Proceedings* 71 no. 4 (2014-2015): 12-14. http://uscgproceedings.epubxp.com/i/436751-win-2015.

Office of Cyber and Infrastructure Analysis (OCIA), “Consequences to Seaport Operations from Malicious Cyber Activity,” March 3, 2016, http://www.maritimedelriv.com/Port_Security/DHS/DHS_Files/OCIA_Consequences_to_Seaport_Operations_from_Malicious_Cyber_Activity.pdf.

Oldman, Kit. “Employers lock out Longshore Workers at West Coast Ports on September 27, 2002.” *Historylink.org*, July 17, 2008. http://www.historylink.org/index.cfm?DisplayPage=output.cfm&file_id=8692.

Paganini, Pierluigi. “U.S. Ports Are Still Vulnerable to Cyberattacks That Release Dangerous Chemicals, Cybersecurity in the Maritime Industry is Crucial for Homeland Security.” *Security Affairs*, October 12, 2015. http://securityaffairs.co/wordpress/40960/security/us-ports-vulnerable-hacking.html.

Peterson, Peterson. “Why Naval Academy Students are Learning to Sail by the Stars for the First Time in a Decade.” *The Washington Post*, February 17, 2016. https://www.washingtonpost.com/news/the-switch/wp/2016/02/17/why-naval-academy-students-are-learning-to-sail-by-the-stars-for-the-first-time-in-a-decade/.

Port of Beaumont. “Our Facilities.” Accessed March 25, 2016. http://www.portofbeaumont.com/.

Port of Houston. "Foreign Trade Statistics.” Accessed March 22, 2016. http://www.portofhouston.com/static/gen/inside-the-port/Communications/Factsheets/FTS_Tonnage_Cargo_2013.pdf.

Port of Long Beach. "Yearly TEUs." Accessed March 23, 2016. http://www.polb.com/economics/stats/yearly_teus.asp.

———. “Port of Long Beach Strategic Plan 2016,” accessed March 29, 2016. http://www.polb.com/civica/filebank/blobdload.asp?BlobID=12848.

Port of Los Angeles, “Port of Los Angeles Earns 19 Awards for Cyber Security Operations Center, Communication Initiatives,” November 24, 2014, https://www.portoflosangeles.org/newsroom/2014_releases/news_112414_AAPA_Awards.asp.

———. "TEU Statistics (Container Counts)." Accessed March 23, 2016. https://www.portoflosangeles.org/maritime/stats.asp.

———."Agreement between the City of Los Angeles Harbor Department and Accuvant, Inc. for a Cyber Security Operations Center, Phase 1." October 16, 2013. https://www.portoflosangeles.org/Board/2013/November%202013/110713_Item_15_Board_Report.pdf.

———. "Cyber Security Operations Center Summary."Accessed March 23, 2016. http://aapa.files.cms-plus.com/Port%20of%20LA%20SUMMARY%20-%202014%20AAPA%20IT%20Award.pdf.

Roberts, John. "Exclusive: GPS Flaw Could Let Terrorists Hijack Ships, Planes." *Fox News*, July 26, 2013. http://www.foxnews.com/tech/2013/07/26/exclusive-gps-flaw-could-let-terrorists-hijack-ships-planes.html.

Scullin, Sara. "Order in the Port." *Law Enforcement Technology* (April 2015): 27–28. http://let.epubxp.com/i/488815-apr-2015/26.

Smith, Greg. "Combating Inside Threat: The greatest Threats are the Ones with Access." *Coast Guard Proceedings* 71, no. 4 (2014–2015): 69-71. http://uscgproceedings.epubxp.com/i/436751-win-2015.

Sturgis, Linda A, Tiffany C. Smythe, and Andrew E. Tucci. "Port Recovery in the Aftermath of Hurricane Sandy: Improving Port Resiliency in the Era of Climate Change." Center for a New American Security. August 2014. http://www.cnas.org/sites/default/files/publications-pdf/CNAS_HurricaneSandy_VoicesFromTheField.pdf.

Swanbeck, Sonja. "Coast Guard Commandant Addresses Cybersecurity Vulnerabilities on Offshore Oil Rigs." *CSIS Strategic Technologies Program*, June 22, 2015. http://www.csis-tech.org/blog/2015/6/22/coastguard-commandant-addresses-cybersecurity-vulnerabilities-in-offshore-oil-rigs.

Szakonyi, Mark. "U.S. Coast Guard Takes Lead to Address Cyber Risks at Ports." *JOC.com*, April 1, 2015. http://www.joc.com/regulation-policy/transportation-policy/us-transportation-policy/us-coast-guard-takes-lead-address-cyber-risks-ports_20150401.html.

Thomson, Candy. "Port of Baltimore is Vulnerable to Cyber-attack, Brookings Study Says." *The Baltimore Sun*, July 5, 2013. http://articles.baltimoresun.com/2013-07-05/business/bs-bz-port-security-20130703_1_maryland-port-administration-cybersecurity-port-officials.

Torbati, Yeganeh, and Jonathan Saul. “Iran’s Top Cargo Shipping Line Says Sanctions Damage Mounting.” *Reuters*, October 22, 2012. http://www.reuters.com/article/us-iran-sanctions-shipping-idUSBRE89L10X20121022.

Thompson, Brittany, M. “GPS Spoofing and Jamming: A global Concern For all Vessels.” *Coast Guard Proceedings* 71, no. 4 (2014–2015): 50-51. http://uscgproceedings.epubxp.com/i/436751-win-2015.

United States Maritime Administration (MARAD). “Marine Transportation System (MTS).” Accessed April 9, 2016. http://www.marad.dot.gov/ports/marine-transportation-system-mts/.

United States Coast Guard. *United States Coast Guard Cyber Strategy*. Washington, DC: United States Coast Guard, June 2015. https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf..

U.S. Coast Guard Navigation Center. “Loran-C General Information.” Last modified June 8, 2012. http://www.navcen.uscg.gov/?pageName=loranMain.

U.S. Department of Transportation Maritime Administration, "Foreign-Flag Crewing Practices: A Review of Crewing Practices in U.S.–Foreign Ocean Cargo Shipping," November 2006. http://www.marad.dot.gov/wp-content/uploads/pdf/Crewing_Report_Internet_Version_in_Word-update-Jan_final.pdf.

Vicinanzo, Amanda. “Cyber Attacks Against SCADA Systems Doubled in 2014, Says Dell Threat Report.” *Homeland Security Today*, April 14, 2015. http://www.hstoday.us/single-article/cyber-attacks-against-scada-systems-doubled-in-2014-says-dell-threat-report/ae81a11c6c44f731bfd5ff8ab6f26c88.html .

Walsh, Don. “Oceans - Maritime Cyber Security: Shoal Water Ahead?” *Proceedings Magazine* 14, no. 7 (2015): 88-92. http://www.usni.org/magazines/proceedings/2015-07/oceans-maritime-cyber-security-shoal-water-ahead.

Warren County Port Commission. "Vicksburg-Warren County Port." Accessed March 23, 2016. http://vicksburgedf.org/.

Wilhusen, Gregory C. *Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity* (GAO-16-116T). Washington, DC: U.S. Government Accountability Office, 2015. http://gao.gov/assets/680/672973.pdf.

White House.gov. “Foreign Policy: Cybersecurity.” Accessed April 8, 2016. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity.

Workman, Daniel. “Iran’s Top 10 Exports.” *World’s Top Exports*, August 29, 2015. http://www.worldstopexports.com/irans-top-10-exports/.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California