The Coast Guard’s Complex Cybersecurity Conundrum

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
06-29-2018	FINAL	

4. TITLE AND SUBTITLE

The Coast Guard's Complex Cybersecurity Conundrum

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LCDR Kathryn A. Moretti, USCG

Paper Advisor (if Any): CAPT Donald E. Bader, USCG

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.
Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Since the 1990s, concern regarding the security of computer networks against adversaries has existed in the maritime community. Considering the nation's ports are the economic and transportation gateways to the world, it is imperative that the systems used to facilitate smooth operations in the port environment be secured from outside disruption. The Coast Guard is the regulatory agency charged with ensuring security of the nation's ports, however it is ill-equipped to adequately handle the cybersecurity mission in the ports due to lack of resources, skillsets and clear authorities. The vulnerability of the nation's ports require action now to shore up weaknesses. Given its port security responsibility under the Department of Homeland Security, it is the entity best situated to address the urgent cyber threat and confidently serve as lead federal agency.

15. SUBJECT TERMS

Cyber, Cybersecurity, Coast Guard, Ports, Maritime Transportation System

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		26	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

Contents Page

Abstract

The Coast Guard's Complex Cybersecurity Conundrum

Since the 1990s, concern regarding the security of computer networks against adversaries has existed in the maritime community. Considering the nation's ports are the economic and transportation gateways to the world, it is imperative that the systems used to facilitate smooth operations in the port environment be secured from outside disruption. The Coast Guard is the regulatory agency charged with ensuring security of the nation's ports, however it is ill-equipped to adequately handle the cybersecurity mission in the ports due to lack of resources, skillsets and clear authorities. The vulnerability of the nation's ports require action now to shore up weaknesses. Given its port security responsibility under the Department of Homeland Security, it is the entity best situated to address the urgent cyber threat and confidently serve as lead federal agency.

INTRODUCTION

Cybersecurity is a complex, but not intractable problem. In particular, cybersecurity of America's ports is a challenging issue in which the Coast Guard has a large stake. In 2015, the Coast Guard Commandant, Admiral Paul Zukunft, seized the initiative and issued a Cyber Strategy for the service that set forth strategic goals against the threat of cyber attacks. The conceptual document provides guidance to the service to address the emerging threat of cyber attacks against ports and maritime critical infrastructure. The strategy lays out three priorities for the service: defending cyberspace, enabling operations, and protecting infrastructure.[1] As the Sector Specific Agency (SSA) for maritime transportation, the Coast Guard has responsibility to identify physical threats, ensure protection of ports from attack and regulate industry for security compliance.[2] Therefore, it can claim a naturally-held responsibility for leading the unity of effort in protecting maritime critical infrastructure against cyber threats, as well.

Despite the correlated authorities and the published strategy, tension exists regarding which entity should lead the cybersecurity initiative. The responsibilities and authorities to conduct cybersecurity are spread across many federal entities including the Department of Homeland Security (DHS) and the Department of Defense (DOD). While the debate is ongoing, the need to shore up vulnerabilities and provide a robust cybersecurity plan for the nation's ports is time-sensitive and critical. The Coast Guard is ill-equipped to adequately handle the cybersecurity mission in the ports due to lack of resources, skillsets and clear

[1] U.S. Coast Guard, *USCG Cyber Strategy*, 2015, 11, https://www.overview.uscg.mil/Portals/6/Documents/PDF/CG_Cyber_Strategy.pdf, Accessed 5/1/18.
[2] U.S. Department of Homeland Security and U.S. Department of Transportation, *Transportation Systems Sector-Specific Plan*, 2015, ii, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf, Accessed 5/1/18.

authorities, but given its port security responsibility under the DHS, it is the best option available for addressing this urgent threat and confidently serving as the lead federal agency.

A COMPLEX PROBLEM

Cybersecurity of ports has been a topic of discussion for many years, with assessments of vulnerabilities and suggested courses of remedial action since at least 1996, when addressed in President William Clinton's Executive Order 13010, "Critical Infrastructure Protection."[3] *The Critical Infrastructure Gap: US Port Facilities and Cyber Vulnerabilities*, a 2013 study by then-Commander Joseph Kramek, United States Coast Guard, highlights the knowledge but lack of action by several ports to properly identify cybersecurity as a major priority and threat.[4] The ports are of utmost importance because they are the nation's gateway to the world.

In 2014, a nation-wide study valued United States seaports at almost $4.56 trillion which supported 3.1 million jobs.[5,6] Nearly 95 percent of the world's commodities travel in the maritime environment.[7] Furthermore, six critical infrastructure sectors—critical

---

[3] Kevin P. Newmeyer, "Who should Lead U.S. Cybersecurity Efforts?" *Prism : A Journal of the Center for Complex Operations* 3, no. 2 (03, 2012): 117, http://www.dtic.mil/dtic/tr/fulltext/u2/1042583.pdf, Accessed 5/1/18.

[4] Joseph Kramek, "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities." Center for 21st Century Security and Intelligence at Brookings, 12-22, https://www.brookings.edu/wp-content/uploads/2016/06/03-cyber-port-security-kramek.pdf, Accessed 5/1/18.

[5] National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis, Operational Analysis Division, "Consequences to Seaport Operations from Malicious Cyber Activity," Mar 3, 2016. https://homeport.uscg.mil/Lists/Content/Attachments/2203/OCIA_Consequences%20to%20Seaport%20Operations%20from%20Malicious%20Cyber%20Activity.pdf, Accessed 5/7/18.

[6] Martin Associates, "The 2014 National Economic Impact of the U.S. Coastal Port System" March 2015, 6, http://aapa.files.cms-plus.com/SeminarPresentations/2015Seminars/2015Spring/US%20Coastal%20Ports%20Impact%20Report%202014%20methodology%20-%20Martin%20Associates%204-21-2015.pdf, Accessed 5/13/18.

[7] Jeffrey P. High, "Testimony," House, *U.S. Coast Guard's Maritime Domain Awareness Efforts: Hearing before the Subcommittee on Coast Guard and Maritime Transportation of the Committee on Transportation and Infrastructure*, 108th Cong., 2nd sess., 2004,1.

manufacturing, commercial facilities, food and agriculture, energy, chemical, and transportation systems— rely heavily on American ports and waterways to transport resources and goods that sustain their businesses.[8] The consequences of a cyber attack on a single port, even for only one day, can have a serious impact on the United States' economy. A recent example of the crippling impact was felt by shipping company, Maersk, in June 2017 when a cyber attack forced the company to halt operations in the Port of Los Angeles for five days and disrupted normal operations for nearly two weeks.[9] Port of Los Angeles Executive Director, Eugene Seroka, testified before Congress regarding the impact his port experienced, noted the $300 million cost to Maersk, and highlighted the example as a "call to arms" for better cybersecurity practices.[10] The consequences of failing to address the cybersecurity challenge not only imply a national impact to the six critical infrastructure sectors but also has repercussions in global trade.

The staggering impact of degraded port operations is not a new concern. Following the Maritime Transportation Security Act of 2002 (MTSA), in which Coast Guard Captains of the Port were designated as Federal Maritime Security Coordinators, the Coast Guard became the "lead agency for coordinating all maritime security planning and operations in

---

[8] National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis, Operational Analysis Division, "Consequences to Seaport Operations from Malicious Cyber Activity," 3 Mar 2016, https://homeport.uscg.mil/Lists/Content/Attachments/2203/OCIA_Consequences%20to%20Seaport%20Operations%20from%20Malicious%20Cyber%20Activity.pdf, Accessed 5/7/18.

[9] Jill Leovy, "Cyberattack Cost Maersk as Much as $300 Million and Disrupted Operations for 2 weeks," *LA Times*, 17 Aug 2017, http://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html, Accessed 5/13/18.

[10] Eugene Seroka, "Testimony," House. *Examining Physical Security and Cybersecurity at Our Nation's Ports: Hearing before the Homeland Security Subcommittee on Border and Maritime Security of the Committee on Homeland Security*. 115th Cong., 1st sess., 2017, 3, https://docs.house.gov/meetings/HM/HM00/20171030/106517/HHRG-115-HM00-Wstate-SerokaE-20171030.pdf. Accessed 5/1/18.

our ports and waterways."[11] The American economy relies upon the Coast Guard to protect and regulate the ports in order to sustain the nation's trade routes. While heavy emphasis is placed upon the entities who own the port facilities and the private corporations who operate out of those ports, the Coast Guard is the federal regulatory agency that ensures compliance in accordance with standards.

General port security has been part of the Coast Guard repertoire since WWII, when the Japanese caught the United States by surprise at Pearl Harbor.[12] The act not only highlighted the vulnerability of the port environment, but inspired action to harden ports against future attack. Over time, port security has continuously improved into the comprehensive Ports, Waterways and Coastal Security (PWCS) mission set following MTSA.

Now that the world has gone digital, port *cyber* security is required to protect against nefarious actors as well as ensure compliance with standards. Cybersecurity is defined as "measures taken to protect a computer or computer system against unauthorized access or attack."[13] This paper will focus on cybersecurity of operational technology (OT) in the port, as opposed to information technology (IT). The International Maritime Organization defines OT as those systems "focusing on the use of data to control or monitor physical processes."[14] For example, OT are systems that regulate pumps and valves at an oil refinery, control the

---

[11] U.S. Coast Guard, *Coast Guard Publication 1: Doctrine for the U.S. Coast Guard, Feb 2014*, 15, https://cg.portal.uscg.mil/units/CGRU/Shared%20Documents/JS%20Pubs%20-%20CG%20Pubs%20-%20Reference%20-%20white%20papers/Coast%20Guard%20Pub_1.pdf. Accessed 5/13/18.

[12] William Theisen, "The Long Blue Line: 9/11 and the U.S. Coast Guard," *Coast Guard Compass Blog*, 7 Sep 2017, accessed 13 May 2018, http://coastguard.dodlive.mil/2017/09/the-long-blue-line-911-and-the-u-s-coast-guard/.

[13] Merriam-Webster, "Cybersecurity." https://www.merriam-webster.com/dictionary/cybersecurity, Accessed 5/7/18.

[14] International Maritime Organization, "Guidelines of Maritime Cyber Risk Management," 5 July 2017, http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/ Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20 Risk%20Management%20(Secretariat).pdf. Accessed 5/4/18.

automatic gate surrounding a maritime facility, or allow for the operation of a crane moving containers on an off ships in port. These systems, many of which are highlighted in Figure 1, are often referred to as Industrial Control Systems (ICS).[15]

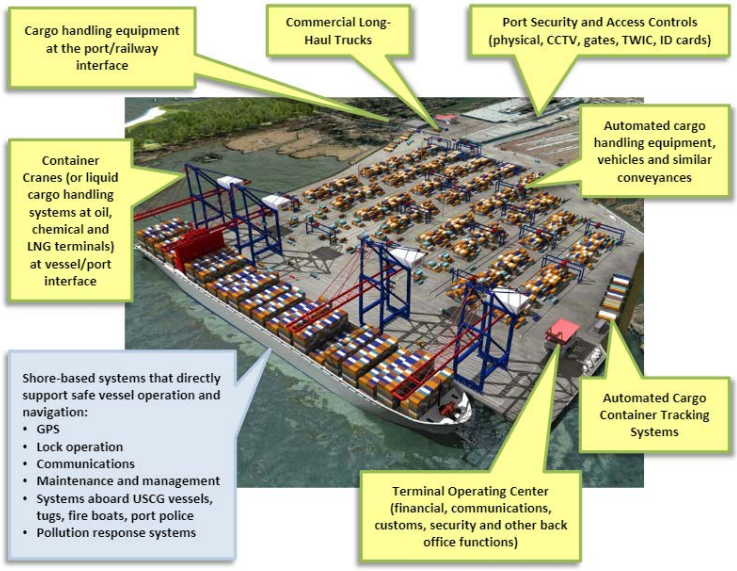

Figure 1: Typical Shore-based, Maritime Transportation Industrial Control Systems[16]

Former President Obama is quoted as saying the cyber threat is "one of the most serious economic national security challenges that we face as a nation."[17] While he was not specifically talking about cybersecurity in the ports, the security of ICS directly impacts the effective management of the port, which has secondary and tertiary effects on the nation's economy. Not only is the United States' Gross Domestic Product impacted if port operations are degraded, but local economies are affected as is the ability to project military power

[15] U.S. Department of Transportation. John A. Volpe National Transportation Systems Center. "ICS Security in Maritime Transportation: A White Paper Examining the Security and Resiliency of Critical Transportation Infrastructure." July 2013. https://rosap.ntl.bts. gov/view/dot/10057. Accessed 5/13/18.
[16] U.S. Department of Transportation. "ICS Security in Maritime Transportation," 11.
[17] Barack Obama, President (address, Cybersecurity and Consumer Protection Summit, Stanford University, Stanford, CA, 13 Feb 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit, Accessed 5/10/18.

globally.[18] Currently, the Coast Guard monitors and inspects the physical aspects of many of these systems to ensure compliance with federal regulations. This paper will focus on the challenges the Coast Guard faces in identifying threats, protecting, and regulating the digital component of the physical systems over which it currently has responsibility.

THE CHALLENGES

Resources

To understand the difficulty of committing resources, one must understand the Coast Guard's current responsibilities. The Coast Guard derives its authorities under Title 14 of the United States Code (USC), which establishes the Coast Guard as both a military service and a law enforcement authority.[19] In order to complete those duties, the Service has 11 statutory missions codified in law under the Homeland Security Act of 2002 which are identified in Table 1.[20]

Table 1: Coast Guard Missions

Homeland Security Missions	Non-Homeland Security Missions
Ports, Waterways and Coastal Security	Marine Safety
Drug Interdiction	Search and Rescue
Migrant Interdiction	Aids to Navigation
Defense Readiness	Living Marine Resources
Other Law Enforcement	Marine Environmental Protection
	Ice Operations

[18] *Maritime Transportation System Security Recommendations for the National Strategy for Maritime Security*, October 2005, ii, https://www.dhs.gov/sites/default/files/publications/HSPD_MTSSPlan_0.pdf. Accessed 5/14/18.
[19] *Establishment of Coast Guard*, U.S. Code, vol. 14, sec. 1, https://www.gpo.gov/fdsys/pkg/USCODE-2010-title14/html/USCODE-2010-title14-partI-chap1-sec1.htm Accessed 5/1/18.
[20] *Homeland Security Act of 2002*, Public Law 107-296, 107th Cong., 2nd sess., 25 November 2002. https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf. Accessed 5/13/18.

As noted previously, port security, now PWCS, has been one of the Coast Guard's missions for over seven decades. However, "security" has always implied physical security and cybersecurity is not even mentioned on the Coast Guard's PWCS information webpage.[21] Not only does cybersecurity appear to be an afterthought in the doctrine, but the service is challenged to accept the responsibility because of funding, time, manning and capacity.

The Coast Guard has a small budget in comparison to its needs, as is common for government agencies. The budget funds the current 11 missions, but not cybersecurity. The Coast Guard requested $11.65 billion to accomplish its missions in Fiscal Year 2019 (FY19).[22] In March 2018, Coast Guard Commandant, Admiral Paul Zukunft, testified before Congress regarding the FY19 request stating the Coast Guard "offers an agile toolset to address the nation's most pressing challenges."[23] However, despite cybersecurity being highlighted as a national security challenge, his testimony addresses cybersecurity only one time—relating to compliance with the Department of Defense Information Network, of which the Coast Guard is a part.[24] While cyber is identified a handful of times in the congressional justification documents that support Admiral Zukunft's testimony, many references are for future research and development (R&D) considerations for internal IT

[21] Office of Counterterrorism & Defense Operations Policy, PWCS https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Response-Policy-CG-5R/Office-of-Counterterrorism-Defense-Operations-Policy-CG-ODO/PWCS/ 5/13/18
[22] https://www.uscg.mil/Portals/0/documents/budget/FY2019BudgetFactSheet_FINAL.PDF 5/13/18
[23] Paul F. Zukunft, Admiral. "Testimony." House. *The Coast Guard's Fiscal Year 2019 Budget Request: Hearing before the House Coast Guard and Maritime Transportation Subcommittee of the Committee on Homeland Security.* 115th Cong., 2st sess., 2018, 8. https://docs.house.gov/meetings/HM/HM11/20151008/104007/HHRG-114-HM11-Wstate-ParsonsR-20151008.pdf. Accessed 5/1/18.
[24] Zukunft, "Testimony," 8.

programs and not immediate implementation of cybersecurity practices for industry OT.[25] Based on the testimony and justification, fiscal resourcing for cyber appears non-existent.

Besides the lack of budget allocation for cyber, time is also sparse. Immediate steps are necessary to harden critical infrastructure against cyber attacks. R&D studies scheduled in future years do not resolve or protect against vulnerabilities, like the Maersk incident, happening now. Unfortunately, building cyber capacity takes time, digital technology evolves quickly, and it is certainly moving faster than the Coast Guard can adapt, particularly considering cybersecurity is not at the forefront of Coast Guard operations now.

Currently in the forefront are the primary missions of 37 multi-missioned Coast Guard Sectors along the coasts, major inland rivers, great lakes, and in US territories.[26] Sectors are tactical level units responsible for "prevention, protection, response and recovery" of the maritime environment in a given geographic location.[27] To that end, manning requirements for each Sector differ depending on the unit's area of responsibility and expected workload. Sectors make up approximately 15 percent of the Coast Guard's more than 47,000 active duty and civilian members.[28] With one or more of the 11 statutory missions to conduct on a daily basis, each Sector member is gainfully employed. Furthermore, less than 0.6 percent of Coast Guard personnel are designated to inspect and regulate port facilities for ICS compliance.[29] These numbers indicate that every position

---

[25] "U.S. Coast Guard Fiscal Year 2019 Congressional Justification," https://www.uscg.mil/Portals/0/documents/budget/FY% 202019%20USCG%20Congressional%20Justification.pdf, Accessed 5/13/18.
[26] U.S. Coast Guard, "Shore Forces."https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf. Accessed 5/14/18.
[27] U. S. Coast Guard, *U.S. Coast Guard Sector Organization Manual* COMDTINST M5401.6A, September 2012, https://cg.portal.uscg.mil/sites/externaldata/Directives/ CIM_5401_6A.pdf, Accessed 5/14/18.
[28] Marty J. Drake, U.S. Coast Guard, "2018-04 EXCEL_PAL," https://cg.portal.uscg.mil/units/cg833/PAL/PAL%20Reports/Forms/AllItems.aspx?RootFolder=%2Funits%2Fcg833%2FPAL%2FPAL%20Reports%2FExcel%20PAL%2FFY18&FolderCTID=0x012000EE023404E1500E42A390094EB7E05A93&View={1B984E1E-9D9C-4E8B-A269-552AA9AF0973}, Accessed 5/14/18.
[29] Drake, "2018-04 EXCEL_PAL."

matters and one particular gap in the Sector organization is the lack of cybersecurity professionals. Although physical security is mentioned in the Sector Organization Manual, "cyber" is not identified in the document.[30]

Whether cyber is mentioned in the guiding documents or not, Coast Guard units' lack of capacity to undertake cyber as a mission remains a glaring concern. The complete allocation of the Coast Guard budget dedicated to other operational requirements and the lack of excess time and manpower to dedicate to cybersecurity indicate the Coast Guard is resource-constrained and ill-equipped to assume the cybersecurity mission.

Skillsets

Until now, the mention of resources has been general: money, time, personnel, and capacity. Perhaps more importantly, the personnel required to do such work must be cyber specialists. In 2009, then-Commandant, Admiral Thad Allan, issued a directive for the development of a service Cyber Command (CGCYBER), which was officially established in July 2013.[31] Furthermore, since the Coast Guard Cyber Strategy was released in 2015, the Commandant, Admiral Paul Zukunft, has more definitively stated the Coast Guard's role by declaring cyberspace an operational domain and identifying a bold strategy for protecting infrastructure.[32] However, the Coast Guard lacks the requisite skillsets to adequately perform cybersecurity in the ports. While CGCYBER's mission is essential to ensuring Coast Guard networks are secure, their focus is primarily inward at the service's IT systems

[30] U.S. Coast Guard, *Sector Organization Manual.*
[31] U.S. Coast Guard, "CGCYBER from the beginning…,"
https://cg.portal.uscg.mil/units/cybercom/SitePages/CGCYBERCOM%20History.aspx, Accessed 5/14/18.
[32] U.S. Coast Guard, "Cyber from the beginning…"

and not outward at either industry IT or OT regulation.[33] The Coast Guard Sectors, which do regulate OT, do not have organic cyber expertise.

Coast Guard Headquarters (CGHQ) recently requested that Sectors identify cyber Subject Matter Experts (SMEs) to provide outreach and training and to serve as points of contact for CGHQ.[34] The lack of criteria for selecting a SME suggests a poor definition of "expertise" and a dearth of consistency. Two logical options for SME appointees are Port Security Specialists (PSS) and Facility Inspectors. PSS responsibility includes conducting risk assessments, facilitating port-wide contingency exercises and managing the Area Maritime Security Committees in the port.[35] Facility Inspector responsibilities include literal inspections, review and approval of security plans, and the conduct of unannounced readiness drills (e.g. the front gate is broken, what are the steps to fix it?)[36] Neither job description includes cybersecurity expertise. Unlike many Coast Guard roles which require personnel to be specialists in their field through schooling and on-the-job training, there is no formal training for these SMEs, with the exception of a PowerPoint presentation.[37] Information gleaned through self-guided PowerPoint training is not generally well-retained. The training does not fully provide the tools SMEs require to protect and regulate against cyber threats. A simple checklist would at least provide some standardization for inspectors across the nation on what to look for in evaluating the completeness of a facility security plan regarding good cybersecurity hygiene measures. However, no checklist currently exists for cyber.[38] Although, Congress recently passed a resolution for the Coast Guard to create a cyber risk

[33] U.S. Coast Guard, "Cyber from the beginning…"
[34] U.S. Coast Guard Port Security Specialist phone interview, 3 May 2018.
[35] Port Security Specialist phone interview.
[36] Port Security Specialist phone interview.
[37] Port Security Specialist phone interview.
[38] Port Security Specialist phone interview.

assessment model, the tool to conduct such assessments is not yet developed for PSS use.[39] Thus, Coast Guard PSS and Inspectors are left to their own devices, and Coast Guard units are reliant upon their organic knowledge base to ensure adequate infrastructure protection.

Not only does the Coast Guard currently lack the knowledge and tools, but the promise of attracting cyber talent is dim. The military is notorious for having difficulty recruiting and retaining talent in fields that are in high demand in the private sector.[40] In particular, the competition between government and the private sector for cyber talent is tough when private industry has unlimited bankroll potential. While agencies like NSA and FBI have had success filling cybersecurity positions, other agencies are not as popular. Furthermore, the government is often hamstrung by its own talent management practices: the cumbersome civilian hiring process and military experience developed through the ranks. The Army is currently testing a pilot program to direct commission cyber talent.[41] The concept is admirable but controversial because candidates will essentially bypass military indoctrination required of traditional forces. However, if the program works, it will be a recruiting model for the Coast Guard to consider.

Even if the Coast Guard was full of cyber experts and could retain them, there is no Standard Operating Procedure for OT cybersecurity. The Coast Guard's 2015 Cyber Strategy is a conceptual document which expresses the Commandant's priorities for cyber.[42] It does not provide operational or tactical guidance on how to conduct the cyber mission. Until clear guidance is established, the cybersecurity mission will be difficult to achieve.

---

[39] Port Security Specialist phone interview.
[40] Kevin P. Newmeyer, "Who should Lead U.S. Cybersecurity Efforts, 117.
[41] David Vergun, "Army to direct commission cyber officers." *Army News Service*, December 4, 2017, https://www.army.mil/article/197691/army_to_direct_commission_cyber_officers. Accessed 5/4/18
[42] U.S. Coast Guard, *USCG Cyber Strategy*, 2015.

Authorities

Securing ports against cyber attacks is difficult because of a deficiency in clear legal authorities. Furthermore, there are overlaps and gaps in current authorities. In 2013, Kramek said the CG needed clearly defined authorities to regulate cyber security.[43] Two years later, a Government Accountability Office report recommended DHS direct the Coast Guard to account for cybersecurity in their next risk assessment cycle.[44] While DHS, and by extension the Coast Guard, protects the homeland; the Department of Defense (DOD), specifically US Northern Command (NORTHCOM), does also.[45]

NORTHCOM's mission statement includes conducting homeland defense, civil support, and security cooperation.[46] Specifically, NORTHCOM's Cyberspace Operations Directorate "executes cyberspace operations providing a secure, collaborative, information environment"[47] Their missions directly relate to United States' national interests in securing the ports from adversaries. U.S. Naval War College Cybersecurity Professor, Chris Demchek, agrees, suggesting cybersecurity responsibility should lie with the "central locus of computer knowledge," which she claims is the DOD.[48] Although the business of Offensive Cyber Operations (OCO) are clearly within DOD's responsibility, Defensive Cyber Operations (DCO) are a shared responsibility. In fact, legislation mandates DHS responsibility for DCO (e.g. cybersecurity). Furthermore, despite the DOD's maturity and capability relative to cybersecurity, it is restricted by the Posse Comitatus Act and lacks

[43] Joseph Kramek, "The Critical Infrastructure Gap."
[44] Gregory C. Wilshusen, "DHS Needs to Enhance Efforts Efforts to Address Port Cybersecurity," Testimony before Congress. GAO Report. https://www.gao.gov/assets/680/672973.pdf, Accessed 5/14/18.
[45] U.S. NORTHERN COMMAND, "NORAD AND NORTHCOM MISSION DIRECTIVE 1," http://www.northcom.mil/Portals/28/NORAD-USNORTHCOM%20Mission%20Directive%201.pdf?ver=2017-10-24-120040-117, Accessed 5/4/18.
[46] U.S. NORTHERN COMMAND, "MISSION DIRECTIVE 1."
[47] U.S. NORTHERN COMMAND, "MISSION DIRECTIVE 1."
[48] Lecture, Chris Demchek, 5/3/18.

regulatory authority to ensure compliance of DCO actions like private sector cybersecurity. Since knowledge and authorities do not align, the debate exists regarding who should lead the charge. Until the debate is settled, the clear operational authorities remain muddled.

As its title suggests, DHS is focused on securing the nation from adversary attack. In order to achieve that for cyber, it created the National Protection and Policy Directorate (NPPD) to "lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure"[49] in concert with public, private, and government sectors. From its mission statement, and considering ports are critical infrastructure, NPPD appears to be the cyber lead. However, as DHS's executive agent for maritime security, evidenced by its role as SSA for maritime transportation, the Coast Guard is also responsible for cyber security of maritime critical infrastructure. The difference, however, is NPPD—which is the subject of a bill to be reorganized and renamed the Cybersecurity and Infrastructure Security Agency (CISA)—creates policy and monitors cyber events in the National Cybersecurity and Communications Integration Center, but has very little operational interaction in the field.[50] The Coast Guard, on the other hand, is specified as a regulatory agency for port security and conducts the field mission daily across the nation. Thus, the 2015 CG Cyber Strategy logically extended the Coast Guard's authority to include cyber security as well. Even within DHS, the "lead" is unclear, particularly if/when the Cybersecurity and Infrastructure Security Agency is established.

---

[49] National Protection and Programs Directorate. "NPPD at a Glance." https://www.dhs.gov/sites/default/files/publications/nppd-at-a-glance-bifold-02132018-508.pdf. Accessed 5/6/18.

[50] *Cybersecurity and Infrastructure Security Agency Act of 2017*. Public Law 107-296. 107th Cong., 2nd sess., 25 November, https://www.congress.gov/bill/115th-congress/house-bill/3359. Accessed 5/1/18.

THE COAST GUARD OPTION

While DOD and DHS have separate authorities relating to cybersecurity, they have a common thread, namely the Coast Guard. As a branch of the military and an armed service, the Coast Guard has close ties to DOD and collaborates well, and often, with its sister services. Similarly, after several department changes throughout its history, the Coast Guard is situated well within DHS to carry out its military, law enforcement, and regulatory missions in the defense of the homeland. Despite the concerns with equipping the Coast Guard appropriately, it is the agency best suited for the task of port cybersecurity.

If the Coast Guard is in a good position to be the primary agency because cybersecurity falls in line with current missions, actions must be taken to remove the challenged previously discussed. For nearly 218 years, the Coast Guard has risen to the challenge to combat emerging threats to United States ports. Although cybersecurity is a difficult problem, it is not the first time the Coast Guard has adapted to new threats. However, adapting takes time. In this situation, the Coast Guard is at a disadvantage because funding, capacity and ready-made cyber Coast Guardsmen are few and far between.

In 2015, when questioned during a Congressional hearing as to whether or not the Coast Guard was capable of completing the mission, Rear Admiral Paul Thomas said, "We don't view this as a new mission, we view this as a natural extension of our existing missions."[51] While the statement is endearing, doubt still remains. A GAO study from the prior year found that DHS, and by extension the Coast Guard, was slow to engage.[52] Indeed, the House passed a bill in 2017 directing the Coast Guard to create a risk assessment model

[51] Tom Leithauser, "Coast Guard Official tries to dispel doubts about Guard's cyber mission," Cybersecurity Policy Report, Oct 12, 2015: 1. https://search.proquest.com/docview/1724872358?accountid-322.
[52] Tom Leithauser, "Coast Guard Official tries to dispel doubts about Guard's cyber mission,"

for cyber based on National Institute of Standards and Technology framework.[53] Considering that cybersecurity of critical infrastructure was identified as "high risk" in 2003 and 15 years later there still no risk assessment standard, it is fair to say there is doubt that the Coast Guard can handle another requirement in its daily repertoire.[54]

The Coast Guard operates under 14 U.S. Code § 2 - Primary duties; which requires the Coast Guard to conduct its assigned maritime duties and "all matters not specifically delegated by law to some other executive department."[55] If cyber is a matter not specifically delegated to another department and is viewed as an extension of the Coast Guard's current missions, then the Coast Guard must make the effort to definitively assume the leadership role.

Mr. Randy Parsons, Director of Security Services in the Port of Long Beach, testified before Congress affirming the Coast Guard suitability to lead the maritime cybersecurity effort.[56] His opinion is supported by Mr. Seroka's testimony suggesting that although not explicitly stated, the Maritime Safety Transportation Act (MTSA) which guides the Coast Guard in regulating facilities is flexible enough to include cyber.[57] Considering 14 U.S. Code § 2 implied authorities, public sector support, and the Service's initiative with the Cyber Strategy, the next step is to operationalize the intent.

---

[53] House passes cybersecurity bill; maritime advisory committee reviews CG initiatives testimony
[54] Tom Leithauser, "Coast Guard Official tries to dispel doubts about Guard's cyber mission," Cybersecurity Policy Report, Oct 12, 2015: 1. https://search.proquest.com/docview/1724872358?accountid-322.
[55] https://www.law.cornell.edu/uscode/text/14/2 5/11/18, but probably want to also look at actual US CODE
[56] Randy Parsons, "Testimony,"House. *Protecting Maritime Facilities in the 21st Centruy: Are Our Nation's Ports At Risk for Cyber Attack?: Hearing before the Homeland Security Subcommittee on Border and Maritime Security of the Committee on Homeland Security.* 114th Cong., 1st Session., 2015. https://docs.house.gov/meetings/HM/HM11/20151008/104007/HHRG-114-HM11-Wstate-ParsonsR-20151008.pdf. Accessed 5/1/18.
[57] Testimony of E. Seroka, "House Homeland Security Subcommittee on Boarder and Maritime Security Hearing"

Resource Solutions

As Admiral Zukunft's budget testimony revealed, the Coast Guard's overarching fiscal priorities in FY19 do not include cybersecurity. While money fixes many things, immediate concerns regarding the cyber workforce can be addressed without an Act of Congress: namely established doctrine, more effective training for existing forces, and a recruiting campaign for the future Cyber Coastguardsman. Although budgeting for cybersecuirty can be delayed initially by making other changes, time cannot. Time is of the essence and the sooner the Coast Guard commits to leading the cybersecurity effort, the better for its workload and the future of the nation.

Bolstering Skillsets

The absence of established doctrine for cybersecurity can be easily rectified within the policy offices at CGHQ. Written policy to establish a standard for field operators is the first step toward excellence. In addition to Port Security and Facilities program offices working together at CGHQ, staff officers can collaborate with cyber experts within DOD as well as private sector partners.

Along with policy, formalized training for facility inspectors who review security plans can include cybersecurity as a module during required training courses. Additionally, cybersecurity tasks can be included in the Performance Qualification Standards book for validation of on-the-job training. This way, front line responders can immediately bridge the gap between current day inspectors and the cybersecurity experts the Coast Guard plans to acquire in the future.

While training is imperative to ensure facility inspectors have some level of knowledge, cybersecurity expertise is preferred. In that case, a campaign to specifically target candidates with technical backgrounds in computer science and information systems should be a high priority for CG Recruiting Command. Often Coast Guard members are asked to speak in their local communities at school career days and fairs or at boys and girls clubs, thus talking points to help focus cyber recruiting efforts would be beneficial.

Clarifying Authorities

Even more important than cybersecurity expertise is the need for clear authority to lead the effort. The Coast Guard already holds responsibility for port security, all that is left is for DHS to definitively assign the CG as the cybersecurity lead. The "lead" title will give the CG additional legitimacy and an ability to better exercise security over OT, however will not preclude it from capitalizing on the expertise of interagency partners. In particular, DHS's advanced cyber expertise within NPPD would be welcome in an interagency port cybersecurity environment. Current port security programs like the Maritime Transportation System and Maritime Domain Awareness are examples of CG-led efforts that capitalize on private industry, public sector, and government agency capabilities and are examples of how port cybersecurity can be structured under Coast Guard leadership.[58]

CONCLUSION

The difference between a cyber problem and a cybersecurity issue is the presence of an adversary, according to *Cybersecurity and Cyberwarfare: What Everyone Needs to*

[58] Interview with Jeffrey High, May 12, 2018.

Know.[59] For example, a simple malfunction of OT is an unfortunate problem whereas an intentional attack on OT by an adversary is a cybersecurity issue.[60] As more cybersecurity issues arise, the need for the United States to harden its ports against attacks becomes more critical each day. While problems are the responsibility of the private sector entity to correct, the need to protect the United States' ports against attack is the responsibility of the Coast Guard whose role is to protect maritime critical infrastructure.

The current state of the Coast Guard is such that the organization is ill-equipped today to accept responsibility for port cyber security due to limitations in resources, skillsets and authorities. Given its unique position of straddling the lines between military and homeland security, it is the best choice for the lead role in cybersecurity. DOD often provides resource support when its interests align with Coast Guard interests, which they do regarding cybersecurity. In addition, the Coast Guard's regulatory authority over private industry and the close relationships the service and DHS have built over time ensure a unity of effort to defend against cyber threats. Until, and unless another agency develops the interoperability characteristic of the Coast Guard, the service will continue to be the best suited and uniquely positioned cybersecurity force for the maritime environment.

[59] Peter W. Singer and Allan Friedman, *Cybersecurity: What Everyone Needs to Know* (New York: Oxford University Press, 2013), 34.
[60] Singer and Friedman, *Cybersecurity,* 34.

BIBLIOGRAPHY

Barrett, Matthew. "Webcast: Cyber Security Framework Version 1.1." National Institute for Standards and Technology. https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview. Accessed 5/14/18.

Drake, Marty J.U.S. Coast Guard. "2018-04 EXCEL_PAL." https://cg.portal.uscg.mil/units/cg833/PAL/PAL%20Reports/Forms/AllItems.aspx?RootFolder=%2Funits%2Fcg833%2FPAL%2FPAL%20Reports%2FExcel%20PAL%2FFY18&FolderCTID=0x012000EE023404E1500E42A390094EB7E05A93&View={1B984E1E-9D9C-4E8B-A269-552AA9AF0973}. Accessed 5/14/18.

Establishment of Coast Guard. U.S. Code. Vol. 14, sec. 1-2 (1915), https://www.gpo.gov/fdsys/pkg/USCODE-2010-title14/html/USCODE-2010-title14-partI-chap1-sec1.htm Accessed 5/1/18.

Homeland Security Act of 2002. Public Law 107-296. 107th Cong., 2nd sess., 25 November 2002. https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf. Accessed 5/13/18.

International Maritime Organization. "Guidelines of Maritime Cyber Risk Management," 5 July 2017. http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf. Accessed 5/4/18.

Kramek, Joseph. "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities." Center for 21st Century Security and Intelligence at Brookings. https://www.brookings.edu/wp-content/uploads/2016/06/03-cyber-port-security-kramek.pdf. Accessed 5/1/18.

Leiderhauser, Tom. "Coast Guard Official tries to dispel doubts about Guard's cyber mission." Cybersecurity Policy Report, Oct 12, 2015: 1. https://search.proquest.com/docview/1724872358?accountid-322. Accessed 5/1/18.

Martin Associates. "The 2014 National Economic Impact of the U.S. Coastal Port System." March 2015. http://aapa.files.cms-plus.com/SeminarPresentations/2015Seminars/2015Spring/US%20Coastal%20Ports%20Impact%20Report%202014%20methodology%20-%20Martin%20Associates%204-21-2015.pdf. Accessed 5/13/18.

"Rep Mike McCaul: 'Its taking too long to authorize NPPD'", cyberscoop.com. https://www.cyberscoop.com/mike-mccaul-nppd-cybersecurity/. Accessed 5/46/18.

Newmeyer, Kevin P. "Who should Lead U.S. Cybersecurity Efforts?" *Prism : A Journal of the Center for Complex Operations* 3, no. 2 (03, 2012): 115-126. http://www.dtic.mil/dtic/tr/fulltext/u2/1042583.pdf. Accessed 5/1/18.

Obama, Barack, President, United States. Address, Cybersecurity and Consumer Protection Summit, Stanford University, Stanford, CA, 13 Feb 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit. Accessed 5/10/18.

Singer, Peter W., and A. Friedman. *Cybersecurity: What Everyone Needs to Know*. New York: Oxford University Press, 2013.

U.S. Coast Guard. *USCG Cyber Security Strategy, 2015*. https://www.overview.uscg.mil/Portals/6/Documents/PDF/CG_Cyber_Strategy.pdf. Accessed 3/7/18.

U. S. Coast Guard. *U.S. Coast Guard Sector Organization Manual* COMDTINST M5401.6A, September 2012. https://cg.portal.uscg.mil/sites/externaldata/Directives/CIM_5401_6A.pdf.

U.S. Coast Guard. *Coast Guard Publication 1: Doctrine for the U.S. Coast Guard, Feb 2014*. https://cg.portal.uscg.mil/units/CGRU/Shared%20Documents/JS%20Pubs%20-%20CG%20Pubs%20-%20Reference%20-%20white%20papers/Coast%20Guard%20Pub_1.pdf. Accessed 5/13/18.

U.S. Congress. House. *Examining Physical Security and Cybersecurity at Our Nation's Ports: Hearing before the Homeland Security Subcommittee on Border and Maritime Security of the Committee on Homeland Security.* 115th Cong., 1st Session., 2017. https://docs.house.gov/meetings/HM/HM00/20171030/106517/HHRG-115-HM00-Wstate-SerokaE-20171030.pdf. Accessed 5/1/18.

U.S. Congress. House. *Protecting Maritime Facilities in the 21st Centruy: Are Our Nation's Ports At Risk for Cyber Attack?: Hearing before the Homeland Security Subcommittee on Border and Maritime Security of the Committee on Homeland Security.* 114th Cong., 1st Session., 2015. https://docs.house.gov/meetings/HM/HM11/20151008/104007/HHRG-114-HM11-Wstate-ParsonsR-20151008.pdf. Accessed 5/1/18.

U.S. Congress. House, *U.S. Coast Guard's Maritime Domain Awareness Efforts: Hearing before the Subcommittee on Coast Guard and Maritime Transportation of the Committee on Transportation and Infrastructure*, 108th Cong., 2nd sess., 2004. Accessed 5/17/18.

U.S. Congress. House. *The Coast Guard's Fiscal Year 2019 Budget Request: Hearing before the House Coast Guard and Maritime Transportation Subcommittee of the Committee on Homeland Security.* 115th Cong., 2st Session., 2018. https://docs.house.gov/meetings/HM/HM11/20151008/104007/HHRG-114-HM11-Wstate-ParsonsR-20151008.pdf. Accessed 5/1/18.

U.S. Department of Homeland Security. Command, Control, and Interoperability Center for Advanced Data Analytics (CCICADA). "Cyber Attacks on Ports and Ships Could Be Catastrophic, Symposium Speaker Says." http://ccicada.org/2015/03/10/cyber-

attacks-on-ports-and-ships-could-be-catastrophic-symposium-speakers-say/. Accessed 3/7/18.

U.S. Northern Command. "NORAD AND NORTHCOM MISSION DIRECTIVE 1." http://www.northcom.mil/Portals/28/NORAD-USNORTHCOM%20Mission%20Directive%201.pdf?ver=2017-10-24-120040-117. Accessed 5/4/18.

_____. *Maritime Transportation System Security Recommendations for the National Strategy for Maritime Security*. October 2005. https://www.dhs.gov/sites/default/files/publications/HSPD_MTSSPlan_0.pdf. Accessed 5/14/18.

Wilshusen, Gregory C. "DHS Needs to Enhance Efforts Efforts to Address Port Cybersecurity." Testimony before Congress. GAO Report. https://www.gao.gov/assets/680/672973.pdf. Accessed 5/14/18.

_____. National Protection and Programs Directorate. "NPPD at a Glance." https://www.dhs.gov/sites/default/files/publications/nppd-at-a-glance-bifold-02132018-508.pdf. Accessed 5/6/18.

_____. National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis, Operational Analysis Division. "Consequences to Seaport Operations from Malicious Cyber Activity." Mar 3, 2016. https://homeport.uscg.mil/Lists/Content/Attachments/2203/OCIA_Consequences%20to%20Seaport%20Operations%20from%20Malicious%20Cyber%20Activity.pdf. Accessed 5/7/18.

_____. *Transportation Systems Sector Cybersecurity Framework Implementation Guide, June 26, 2015*. https://www.dhs.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf. Accessed 3/7/18.

_____. "U.S. Coast Guard Fiscal Year 2019 Congressional Justification." https://www.uscg.mil/Portals/0/documents/budget/FY%202019%20USCG%20Congressional%20Justification.pdf. Accessed 5/13/18.

_____. U.S. Coast Guard. "CGCYBER from the beginning…." https://cg.portal.uscg.mil/units/cybercom/SitePages/CGCYBERCOM%20History.aspx. Accessed 5/14/18.

_____. U.S. Coast Guard. "Shore Forces."https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf. Accessed 5/14/18.

_____. U.S. Computer Readiness Team. *National Cybersecurity Incident Response Plan.* December 2016. https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf. Accessed 5/14/18.

U.S. Department of Homeland Security and U.S. Department of Transportation. "Transportation Systems Sector-Specific Plan." 2015.

https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf Accessed 5/1/18.

U.S. Department of Transportation. John A. Volpe National Transportation Systems Center. "ICS Security in Maritime Transportation: A White Paper Examining the Security and Resiliency of Critical Transportation Infrastructure." July 2013. https://rosap.ntl.bts. gov/view/dot/10057. Accessed 5/13/18.