The Heritage Foundation

ISSUE BRIEF

No. 4353 | FEBRUARY 23, 2015

The U.S. Needs to Secure Maritime Ports by Securing Network Ports

Riley Walters

Maritime connectedness continues to be a key asset for U.S. economic and strategic interests. Threats to port and vessel network systems have long been overshadowed by concerns about kinetic attacks and supply-chain security. All maritime stakeholders remain at risk of cyber intrusion as cyber attackers seek any and all means of accessing maritime networks. Therefore, key measures need to be in place to evolve symbiotically as new threats emerge.

The U.S. Department of Homeland Security (DHS) and maritime stakeholders need to stay ahead of these risks in order to keep trade flow maximized, while avoiding the creation of regulations that may slow trade and hinder business.

Risks for Port Cybersecurity

For all U.S. industries, cybersecurity costs are growing.[1] Cyber attacks on port systems can have a variety of negative effects. The economic losses from port delays or closure can vary in severity. One port's failure negatively affects all connecting regional ports. In 2002, the 11-day closure of 29 ports on the West Coast cost an estimated $11 billion. Northeast ports lost an estimated $50 billion—$1 billion in cargo delays alone—because of Hurricane Sandy in 2012.[2] As labor disputes that began in October 2014 continue in West Coast ports, trade partners in Asia are feeling the effects of undelivered goods.[3]

With port and vessel network systems implementing new technology, stakeholders are moving away from traditional stand-alone systems, and maritime industrial control systems (ICS) are becoming more integrated. While new systems help to streamline production and increase the flow of trade, the number of vulnerabilities in network systems is also increasing. Cyber threat actors continue to find new ways of accessing network systems, through traditional land-line connections, new or pre-existing Wi-Fi ports, and USB-introduced threats, such as installing malware (Stuxnet) or extracting information (Edward Snowden). Vulnerabilities in smaller systems can be exploited to gain access to larger networks—a time-consuming type of attack for the everyday hacktivist, but a credible investment for drug smugglers and nation-state sympathizers.

In September 2014, the Senate Committee on Armed Services reported that Chinese hackers were behind the successful advanced persistent threat (APT) attacks on contractors in U.S. Transportation Command (TRANSCOM), dating as far back as 2008.[4] The military relies on these commercial vessels for strategic and humanitarian contingencies, transporting 95 percent of U.S. Forces' dry cargo annually.[5] According to the report, Chinese military compromised "multiple systems" on a commercial ship contracted by TRANSCOM for logistics routes. Between June 2012 and May 2013, the FBI reported two shipping companies and eight technical service providers of TRANSCOM were victims of cyber intrusion.

This paper, in its entirety, can be found at **http://report.heritage.org/ib4353**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

A report by CyberKeel, a maritime cybersecurity group, later showed how in late 2013 drug smugglers hired hackers to move drugs through the Port of Antwerp, the second largest seaport in Europe and a member of the Cargo Security Initiative since 2011.[6] The hackers bypassed remote terminals to allow release of the containers and deleted the container transportation information—attributing this to "ghost shipping." The report also showed that, if the hackers had wanted, they could have caused severe congestion and port disruption with the information they accessed.

Two Government Accountability Office (GAO) reports in 2014 highlighted the DHS's need to enhance cybersecurity for maritime systems and DHS facilities. Much like the TRANSCOM report, the GAO reports echoed the need to better define cyber threats and to establish how and to which agency cyber threats are to be reported. The reports also raised a concern about the lack of information sharing among agencies—a cyber threat may fall to the DHS, Department of Justice, Department of Transportation, Department of Defense, or any combination, depending on the victim of the attack.

The U.S. Coast Guard (USCG) began taking public comments at the end of 2014 on how to better develop guidance for maritime cybersecurity.[7] The USCG noted past instances of drug smuggling, disgruntled employees sabotaging network systems, and the disruption of an unmanned crane through cyber intrusions of its GPS.[8] U.S. Coast Guard Commander Joseph Kramek reported that cybersecurity awareness and culture at U.S. ports—specifically in the ports of Baltimore, Houston, Los Angeles, Long Beach, Vicksburg, and Beaumont—were relatively low.[9] He recommended that the DHS, along with the USCG and Federal Emergency Management Agency, need to better address port cybersecurity more, while still focusing on kinetic defense.[10] Only in 2014 did the Port Security Grant Program start allowing grants based on cyber vulnerability assessments.[11] While the threat of a physical attack on or through ports still exists, stakeholders need to realize that cyber threats cannot be addressed in the same way as kinetic defense, although cyber attacks can affect kinetic systems.

1. Riley Walters, "Cyber Attacks on U.S. Companies in 2014," Heritage Foundation *Issue Brief* No. 4289, October 27, 2014, http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014.
2. U.S. Department of Transportation, Research and Innovative Technology Administration, "ICS Security in Maritime Transportation: A White Paper Examining the Security and Resiliency of Critical Transportation Infrastructure," July 2013, pp. 6–7, http://ntl.bts.gov/lib/48000/48000/48074/DOT-VNTSC-MARAD-13-01.pdf (accessed February 13, 2015).
3. Chang-Ran Kim, "Japan Automakers Hit Production Snags as U.S. Port Dispute Drags On," Reuters, February 6, 2015, http://www.reuters.com/article/2015/02/06/us-usa-ports-japan-idUSKBN0LA0MR20150206 (accessed February 10, 2015).
4. U.S. Senate, Committee on Armed Services, "Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors," 113th Cong., 2nd Sess., 2014, pp. 9–10, http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf (accessed February 13, 2015).
5. U.S. Transportation Command, "2012 Annual Report," p. 15, http://www.transcom.mil/documents/annual_reports/annual_report.pdf (accessed February 19, 2015).
6. U.S. Department of Homeland Security, Customs and Border Protection, "Best Practice—Port of Antwerp: Information-Sharing Network," February 2014, http://www.cbp.gov/sites/default/files/documents/bulletin_feb2014_antwerp.pdf (accessed February 13, 2015), and CyberKeel, "Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Sea," October 15, 2014, http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf (accessed February 19, 2015).
7. U.S. Coast Guard, "Guidance on Maritime Cybersecurity Standards," *Federal Register*, Vol. 79, No. 243 (December 18, 2014), pp. 75574–75575, https://www.federalregister.gov/articles/2014/12/18/2014-29658/guidance-on-maritime-cybersecurity-standards (accessed February 13, 2015).
8. Lieutenant Jodie Knox, "Guidance on Maritime Cyber Security Standards—Part 3 Cyber Command Remarks," Coast Guard Maritime Commons, January 23, 2015, http://mariners.coastguard.dodlive.mil/2015/01/23/1232015-guidance-on-maritime-cyber-security-standards-part-3-cyber-command-remarks/ (accessed February 13, 2015).
9. Commander Joseph Kramek, "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities," Brookings *Policy Paper*, July 3, 2013, http://www.brookings.edu/research/papers/2013/07/03-cyber-ports-security-kramek (accessed February 13, 2015).
10. U.S. Government Accountability Office, "Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity," GAO-14-459, June 2014, http://www.gao.gov/assets/670/663828.pdf (accessed February 13, 2015).
11. U.S. Department of Homeland Security, Federal Emergency Management Agency, "FY 2014 Port Security Grant Program (PSGP)," July 25, 2014, http://www.fema.gov/media-library-data/1406300857129-09e62587b8f79e748c585e37cdba09a9/PSGP_Fact%20Sheet_Final.pdf (accessed February 13, 2015).

What Should Be Done

Congress should:

- **Readdress legislation on increasing cyber information sharing.** The DHS and the U.S. Computer Emergency Readiness Team (US-CERT) have taken the lead on cyber information sharing in the past. As they continue to lead, all stakeholders need to agree on threat-defining language. Port stakeholders across federal departments, agencies, and private businesses need to increase cyber information sharing and the ease with which information is shared. The President's recent executive order highlights the importance of information sharing, but falls short in addressing liability risks.[12] Increasing cyber information sharing includes working with international partners because cyber attackers may enter U.S. port networks by any available means. Domestically, agencies should address continuity and simplicity in identifying cyber threats, such as the definition and severity of threats, attacks, and solutions, while avoiding the creation of catch-all regulation that hinders business.

The Administration should:

- **Include a focus for handling cybersecurity for port security in the new Cyber Threat Intelligence Integration Center (CTIIC).**[13] The recently introduced agency, modeled after the National Counterterrorism Center, aggregates cybersecurity information across government. Cyber attacks can happen in a manner of seconds, which is why simplifying reporting of cyber threats is important, including to which agency the threat is reported and the information to be shared interdepartmentally. This will give stakeholders an advantage in responding to cyber threats.

The DHS should:

- **Continue to work with the Department of Commerce's National Institute of Standards and Technology (NIST) program as the USCG continues to receive public comment on how to address cybersecurity.**

Conclusion

The continued growth of port and network systems is critical for a strong U.S. economic and strategic system. Cyber threats emerge across all network spectrums. While some systems may be considered more critical than others, system administrators need to able to trust that intermediary software, hardware, and connections are also secure. While kinetic defense will always take priority for port and vessel security, cybersecurity should come into focus as the number and severity of cyber attacks continues to grow.

*—**Riley Walters** is a Research Assistant in the Douglas and Sarah Allison Center for Foreign and National Security Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*

12. Barack Obama, "Promoting Private Sector Cybersecurity Information Sharing," Executive Order, February 13, 2015, http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari (accessed February 13, 2015).
13. Steven Bucci, Paul Rosenzweig, and David Inserra, "Q&A: What Is the New Cyber Threat Intelligence Integration Center and How Will It Work?" The Daily Signal, February 11, 2015, http://dailysignal.com/2015/02/11/qa-new-cyber-threat-intelligence-integration-center-will-work/.