CONSEQUENCES TO SEAPORT OPERATIONS FROM MALICIOUS CYBER ACTIVITY

March 3, 2016; 1300 EST

PREPARED BY: OPERATIONAL ANALYSIS DIVISION

SCOPE

The U.S. Department of Homeland Security/Office of Cyber and Infrastructure Analysis (DHS/OCIA) produces Critical Infrastructure Security and Resilience Notes in response to changes in the infrastructure protection community's risk environment from terrorist attacks, natural hazards, and other events. This note examines the potential for malicious actors to use cyber capabilities to disrupt operations at U.S. commercial seaports and the impact major disruptions would have on other critical infrastructure sectors. The networks examined include those used at seaports and aboard vessels. Although this note will mention the previous actions of malicious actors, it will not analyze their current intent and capabilities regarding seaports. In addition, this product will not examine exclusive U.S. Department of Defense and the Defense Industrial Base Sector port facilities. This note supports DHS leadership; federal, state, and local agencies; and private sector partners.

OCIA developed this note in coordination with the DHS/National Protection and Programs Directorate/Office of Infrastructure Protection, DHS/ National Protection and Programs Directorate /Office of Cybersecurity and Communications, DHS/Transportation Security Administration, the DHS/United States Coast Guard, and the United States Maritime Administration.

KEY FINDINGS

- **Unless cyber vulnerabilities are addressed, they will pose a significant risk to port facilities and aboard vessels within the Maritime Subsector. These potential vulnerabilities include limited cybersecurity training and preparedness, errors in software, inadequately protected commercial off-the-shelf technologies and legacy systems, network connectivity and interdependencies, software similarities, foreign dependencies, global positioning system jamming-spoofing, and insider threats.**
- **A cyber attack on networks at a port or aboard a ship could result in lost cargo, port disruptions, and physical and environmental damage depending on the systems affected. The impact to operations at a port, which could last for days or weeks, depends on the damage done to port networks and facilities.**
- **The impacts to critical infrastructure sectors depend on how a cyber attack affects a port, the level and length of disruption that occurs at the port, and the capability to divert shipments to other ports. Although all sectors rely to some degree on the goods that transit U.S. ports, those most likely to be affected by a port disruption are the Critical Manufacturing, Commercial Facilities, Food and Agriculture, Energy, Chemical, and Transportation Systems. If more than one port is disrupted concurrently by a cyber attack, a greater impact to other sectors of critical infrastructure is likely to occur.**
- **Several mitigation measures can increase the security and resiliency of ports: setting up maritime cybersecurity standards, sharing information across the sector, conducting routine vulnerability assessments, using best practices, mitigating insider threats, and developing contingency plans for cyber attacks.**

SEAPORTS OVERVIEW

In the United States and its territories, approximately 3,200 cargo and passenger handling facilities are located within 360 commercial ports. Of these, about 150 are deep water seaports administered by 126 public seaport agencies.[1,2] These ports are located on the Atlantic, Pacific, and Gulf coasts; the Great Lakes; Alaska; Hawaii; and American territories.

The primary role of seaports is to facilitate the movement of trade to both foreign and domestic markets. In 2013, more than 1.1 billion short tons of domestic trade and more than 1.2 billion short tons of foreign trade moved through U.S. ports.[3] Seaports can be broken down into two categories based on how they operate:

- "Landlord" ports, such as the Ports of Los Angeles and Long Beach, build the wharves and rent or lease them to terminal operators who operate cargo-handling equipment and negotiate contracts with shipping companies to load and unload cargo ships.
- "Operating" ports, such as the Port of Charleston, build the wharves, own the cargo-handling equipment, and hire the labor to move cargo within the port.[4]

In 2013, oceangoing vessels made 74,188 calls at ports in the United States. Of these calls, 28,679 were tanker ships, 17,540 were container ships, 12,648 were bulk ships, 5,292 were roll-on roll-off (Ro-Ro) ships, 8,241 were general ships, and 1,788 were gas ships.[5] Cargo and vessel types vary in size and capability.

- **Bulk carriers** transport large quantities of unpackaged cargo. Dry bulk includes products such as corn, grain, coal, and iron ore. Liquid bulk includes chemicals and petroleum products. Break bulk consists of goods shipped in neither containers nor bulk. This includes items shipped in bags and barrels, as well as industrial items, such as steel girders.
- **Container ships** carry intermodal containers: standardized, reusable steel boxes used to store and transport materials. First used in 1956, the intermodal container has revolutionized product shipping making it more economical, more efficient, and more secure.[6] The most common are 20- and 40-foot containers, with a wide variety in each (e.g., refrigerated, open top, tanks, flatrack). Capacity is measured in 20-foot equivalent units (TEUs), in which one TEU is equal to one standard 20- by 8-foot container.[7]
- **Tanker ships** carry the majority of crude oil imported to the United States.[8] Gas carriers transport liquefied natural gas, liquefied petroleum gas, and other chemical gases.
- **Roll-on Roll-off (Ro-Ro) ships** are vessels designed to carry wheeled cargo, including consumer and commercial automobiles, trailers, and railroad cars. Unlike other cargo, which is lifted on and off a vessel, Ro-Ro vessels have ramps that allow cargo to be rolled on and off.
- **General ships** include general cargo carriers, partial containerships, refrigerated ships, barge carriers, and livestock carriers.

SEAPORT ECONOMICS

Seaports are critical facilities in the export and import of raw and finished goods and in the movement of goods across the United States. According to a 2015 study completed for the American Association of Port Authorities,

[1] American Association of Port Authorities, "U.S. Public Port Facts," www.aapa-ports.org/Industry/content.cfm?ItemNumber=1032, accessed 25 June 2015.
[2] A seaport is a harbor at or accessible to the seacoast that accommodates seagoing vessels. A deep draft harbor is one which is constructed to a depth of more than 45 feet. For definition of deep draft, see U.S. Code, Title 33, § 2241, www.gpo.gov/fdsys/pkg/USCODE-2010-title33/pdf/USCODE-2010-title33-chap36-subchapII-sec2241.pdf, accessed 16 July 2015.
[3] American Association of Port Authorities, "U.S. Port Ranking by Cargo Volume 2013," http://aapa.files.cms-plus.com/Copy%20of%202013%20U%20S%20%20PORT%20RANKINGS%20BY%20CARGO%20TONNAGE%5F1427222227746%5F1.xlsx, accessed 16 July 2015.
[4] American Association of Port Authorities, "Glossary of Maritime Terms," www.aapa-ports.org/Industry/content.cfm?ItemNumber=1077, accessed 14 September 2015.
[5] Maritime Administration, "2013 Vessel Calls in U.S. Ports and Terminals–Privately-owned, oceangoing merchant vessels over 1,000 gross tons," U.S. Department of Transportation, www.marad.dot.gov/wp-content/uploads/xlsx/DS_U.S.-Port-Calls-2013.xlsx, accessed 6 October 2015.
[6] Levinson, Marc, "Container Shipping and the Economy," TR News, Transportation Research Board of the National Academies, September–October 2006, pp. 10-13, http://onlinepubs.trb.org/onlinepubs/trnews/trnews246.pdf, accessed 25 June 2015.
[7] The measurement used is an approximation; it takes into account only length and width, not height.
[8] American Petroleum Institute, "Tankers: Fueling American Life," 2011, www.api.org/~/media/files/oil-and-natural-gas/tankers/tankers-lores.pdf, accessed 25 June 2015.

seaports in the United States had a total economic value in 2014 of $4.56 trillion. Of this, $124.45 billion was direct business revenue, and $4.3 trillion was the economic value created by the movement of cargo through seaports.[9] About 95 percent of foreign trade with the United States is moved by ship.[10,11] As of 2014, more than 23 million jobs were supported by cargo moving through seaports, including more than 541,000 jobs directly generated by marine cargo and vessel activity.[12]

While a large number of ports exist, a small subset of ports dominates trade in each of the vessel types. In 2013, by value of trade, the 25 largest seaports accounted for approximately 85 percent of all waterborne foreign trade in the United States.[13] In 2011, the top 10 ports for vessel calls for each type of ship accounted for more than half of all vessel calls in the United States.[14] For example, the top five container ports in the United States in 2014—Los Angeles, Long Beach, New York-New Jersey, Seattle-Tacoma, and Savannah—moved almost as many containers as the next 45 largest container ports combined.[15]

Although ports move numerous types of goods, U.S. ports often specialize in certain commodities. For example, in 2013, ports along the Mississippi Gulf accounted for 48.7 percent of all grain exports by tonnage in the United States; ports in the Pacific Northwest accounted for another 24.6 percent.[16] The 2014 principal imports at the Port of Los Angeles—the port with the most U.S. container traffic—include furniture, auto parts, apparel, and electronics.[17]

SEAPORT DEPENDENCIES

Seaports in the United States critically depend on the Energy, Communications, and Transportation Systems Sectors for daily operations. Other Sectors are also essential to the functioning of the country's seaports, including the Water and Wastewater Systems, Financial Services, Information Technology (IT), Emergency Services, and Government Facilities.

All critical infrastructure sectors directly or indirectly depend on the imports, exports, and domestic shipping conducted at U.S. seaports. Because of the dominance of certain seaports in specific sectors, cascading impacts on critical infrastructure depend on which seaports are disrupted.

CYBER SYSTEMS AT SEAPORTS

Ports and ships use many information systems and communications technologies for various functions, including navigation, communication, equipment operation, cargo movement and tracking, business operations, and security.[18]

Shipping companies rely on navigation software to safely pilot vessels. An Electronic Chart Display and Information System (ECDIS) is a computer-based navigation tool, used as an alternative to paper navigation charts, which integrates information from the global positioning system (GPS), automatic identification systems, radar, and other

---

[9] Martin Associates, "The 2014 National Economic Impact of the U.S. Coastal Port System," completed for American Association of Port Authorities, 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 22 June 2015.
[10] Maritime Administration, "The Maritime Administration and the U.S. Marine Transportation System: A Vision for the 21st Century," Department of Transportation, November 2007, www.marad.dot.gov/wp-content/uploads/pdf/Vision_of_the_21st_Century_10-29.pdf, accessed 2 October 2015.
[11] National Ocean Service, "How important is the ocean to our economy?," National Oceanic and Atmospheric Administration, http://oceanservice.noaa.gov/facts/oceaneconomy.html, accessed 2 October 2015.
[12] Martin Associates, "The 2014 National Economic Impact of the U.S. Coastal Port System," completed for American Association of Port Authorities, 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 22 June 2015.
[13] American Association of Port Authorities, "U.S. Waterborne Foreign Trade Calendar Year 2013, Port Ranking By Value of Trade," http://aapa.files.cms-plus.com/Statistics/U.S.%20WATERBORNE%20FOREIGN%20TRADE%202013%20PORT%20RANKING%20BY%20CARGO%20VALUE.pdf, accessed 16 July 2015.
[14] U.S. Department of Transportation, Maritime Administration, "2011 U.S. Water Transportation Statistical Snapshot," November 2013, p. 13, www.marad.dot.gov/wp-content/uploads/pdf/US_Water_Transportation_Statistical_snapshot.pdf, accessed 25 June 2015.
[15] American Association of Port Authorities, "NAFTA Region Container Traffic 2014 Port Rankings by TEUs," http://aapa.files.cms-plus.com/Statistics/NAFTA%20REGION%20CONTAINER%20TRAFFIC%20PORT%20RANKING%202014.pdf, accessed 25 June 2015.
[16] USDA, "A Reliable Waterway System Is Important to Agriculture," October 2014, www.ams.usda.gov/sites/default/files/media/Importance%20of%20Waterways%2010-2014.pdf, accessed 15 July 2015.
[17] Port of Los Angeles, "Facts and Figures," www.portoflosangeles.org/pdf/POLA_Facts_and_Figures_Card.pdf, accessed 12 August 2015.
[18] Government Accountability Office, "Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity," June 2014, www.gao.gov/assets/670/663828.pdf, accessed 14 September 2015.

relevant systems to continuously display a vessel's position in relation to land, navigation aids, and hazards.[19] The International Maritime Organization has approved ECDIS (unlike electronic chart systems) to replace traditional paper charts. If an ECDIS ceases to meet requirements—by using unofficial charts or having incorrect user settings—it reverts to an electronic chart system.[20]

Industrial Control Systems (ICSs), including Supervisory Control and Data Acquisition (SCADA) systems and distributed control systems, are used throughout the Maritime Subsector, including the loading, unloading, and transportation of bulk and containerized cargo (Figures 1 and 2, respectively).[21]

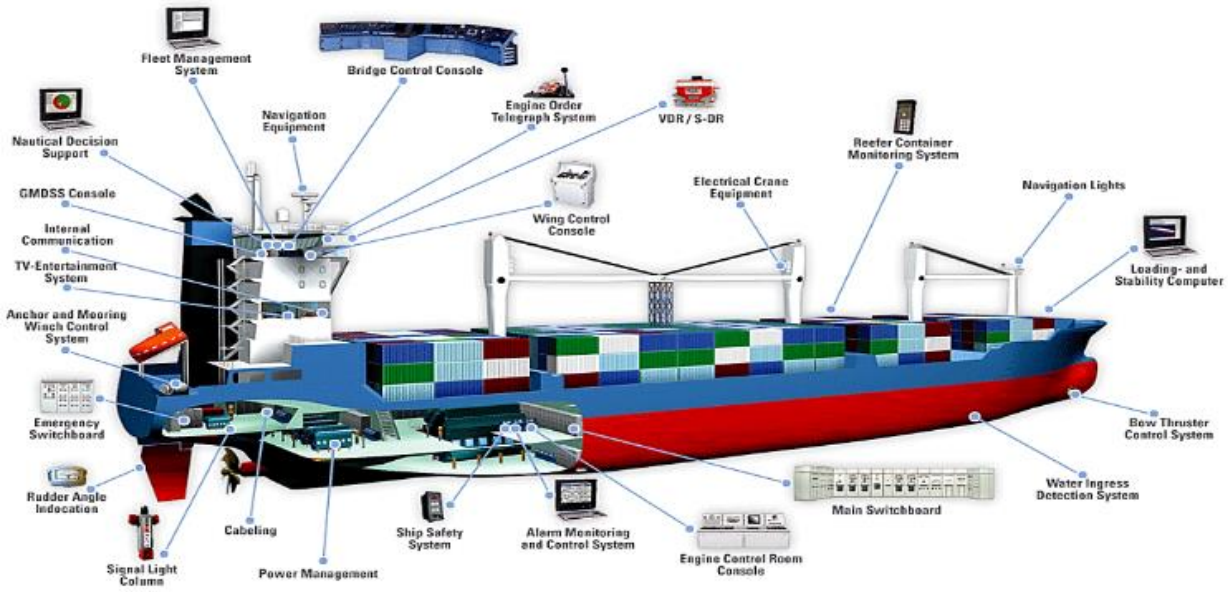

FIGURE 1—TYPICAL SHIPBOARD ICS[22]

[19] Martek Marine Ltd., "About ECDIS," www.ecdis-info.com/about_ecdis.html, accessed 18 September 2015.
[20] ECIDS Ltd., "ECDIS Risk Mitigation," www.ecdis.org/ecdis-risk-mitigation/, accessed 6 October 2015.
[21] John A. Volpe National Transportation Systems Center, "ICS Security in Maritime Transportation," Department of Transportation, July 2013, http://ntl.bts.gov/lib/48000/48000/48074/DOT-VNTSC-MARAD-13-01.pdf, accessed 14 September 2015.
[22] Ibid.

FIGURE 2—TYPICAL SHORE-BASED MARITIME ICS[23]

Terminal operating systems are information systems used by operators to manage the movement and storage of containers inside a terminal. These networks at times are integrated with other systems inside a port, such as financial systems, mobile computing, and radio frequency identification systems with the goal of increasing logistic efficiency.[24]

Business operation systems support a terminal operator's business functions, such as communications with customers, invoice preparation, and billing documentation.[25]

Access control and monitoring systems support physical security operations at U.S. seaports. An example is networked surveillance cameras. These systems are often used for remote monitoring; sensitive areas are often protected by using electronically enabled physical access control devices (e.g., badges).[26,27]

Some wharves and seaports for lease by terminal operators use different cyber systems. Owners of landlord ports at times have little awareness of what networked systems terminal operators run, and they may not know what cybersecurity measures are used to protect these systems.[28] In addition, the physical location of IT systems can vary, as some are managed remotely from locations within and outside of the United States.[29]

SEAPORT CYBER VULNERABILITIES

If unaddressed, cyber vulnerabilities could pose a significant risk in port facilities and aboard vessels within the Maritime Subsector. These potential vulnerabilities include limited cybersecurity training and preparedness, errors

[23] John A. Volpe National Transportation Systems Center, "ICS Security in Maritime Transportation," Department of Transportation, July 2013, http://ntl.bts.gov/lib/48000/48000/48074/DOT-VNTSC-MARAD-13-01.pdf, accessed 14 September 2015.
[24] Government Accountability Office, "Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity," June 2014, www.gao.gov/assets/670/663828.pdf, accessed 14 September 2015.
[25] Ibid.
[26] Commander Joseph Kramek (USCG), "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities," The Brookings Institution, July 2013, www.brookings.edu/~/media/research/files/papers/2013/07/02%20cyber%20port%20security%20kramek/03%20cyber%20port%20security%20kramek.pdf, accessed 14 September 2015.
[27] Government Accountability Office, "Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity," June 2014, www.gao.gov/assets/670/663828.pdf, accessed 14 September 2015.
[28] Commander Joseph Kramek (USCG), "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities," The Brookings Institution, July 2013, www.brookings.edu/~/media/research/files/papers/2013/07/02%20cyber%20port%20security%20kramek/03%20cyber%20port%20security%20kramek.pdf, accessed 14 September 2015.
[29] Government Accountability Office, "Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity," June 2014, www.gao.gov/assets/670/663828.pdf, accessed 14 September 2015.

in software, inadequately protected commercial off-the-shelf technologies and legacy systems, network connectivity and interdependencies, software similarities, foreign dependencies, GPS jamming or spoofing, and insider threats.

LIMITED CYBERSECURITY TRAINING AND PREPAREDNESS

A lack of emphasis on cybersecurity training and preparedness at ports and aboard ships increases cyber vulnerabilities because reduced awareness by personnel increases the potential for malicious activities and limits best practices. Personnel, not properly trained, may unintentionally allow a malicious actor network access through malware delivered through an email, Website, or other means. In addition, affected businesses will likely be less capable of effectively responding to and recovering from malicious cyber activity than a business that maintains a cyber incident response plan.

- A 2013 Brookings Institution study found the level of cybersecurity awareness and culture in U.S. port facilities to be relatively low, and basic cybersecurity measures were often not practiced. The study looked at six commercial ports; only one conducted a cyber vulnerability assessment, and none had a cyber incident response plan.[30,31]
- The same study found that most of these ports did not require cybersecurity training before granting network access to system users.[32] Other groups have found a general lack of awareness of previous cyber incidents and the nature of cyber risks in the Maritime Subsector.[33,34]

INADEQUATELY PROTECTED COMMERCIAL OFF-THE-SHELF TECHNOLOGIES AND LEGACY SYSTEMS

Modern ICSs often use commercial off-the-shelf technologies that are network-based and connected to other systems. In addition, standard operating systems, such as Windows and Linux in ICSs, use has increased.[35] These devices and systems require software updates and replacement when device manufacturers or information security researchers discover technical vulnerabilities, or ICSs become increasingly vulnerable.

Many SCADA systems on ships and in ports are much older than other information systems and were designed before cybersecurity was a common consideration. Despite this, these systems are more likely to be integrated with newer networks for remote access, increasing their exposure to malicious actors. Although reliance on archaic technology can (in a minor way) assist the security of a system because malware or other exploits are not written to compromise older technology, malicious actors who have advanced cyber capabilities could recognize these vulnerabilities and target such older technology.

ERRORS IN SOFTWARE

Errors in the software installed at ports and aboard vessels can have a significant negative impact on maritime operations.

- In 2013, Maher Terminals, which handles a third of the port of New York and New Jersey's volume, experienced significant difficulties after switching to a new computer system at one of its terminals. The impacts at the terminal, which lasted for several weeks, included the closing of the terminal for hours at a time and truck backups lasting 4–6 hours. The problems at the terminal caused significant delays in some

[30] Commander Joseph Kramek (USCG), "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities," The Brookings Institution, July 2013, www.brookings.edu/~/media/research/files/papers/2013/07/02%20cyber%20port%20security%20kramek/03%20cyber%20port%20security%20kramek.pdf, accessed 14 September 2015.
[31] The ports reviewed in the study were Port of Baltimore, Port of Los Angeles, Port of Long Beach, Port of Houston, Port of Vicksburg, and Port of Beaumont.
[32] Commander Joseph Kramek (USCG), "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities," The Brookings Institution, July 2013, www.brookings.edu/~/media/research/files/papers/2013/07/02%20cyber%20port%20security%20kramek/03%20cyber%20port%20security%20kramek.pdf, accessed 14 September 2015.
[33] Cyberkeel, "Maritime Cyber-Risks," October 15, 2014, www.cyberkeel.com/images/pdf-files/Whitepaper.pdf, accessed 8 September 2015.
[34] European Union Agency for Network and Information Security, "Cyber Security Aspects in the Maritime Sector," www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts, accessed 24 September 2015.
[35] John A. Volpe National Transportation Systems Center, "ICS Security in Maritime Transportation," Department of Transportation, July 2013, http://ntl.bts.gov/lib/48000/48000/48074/DOT-VNTSC-MARAD-13-01.pdf, accessed 14 September 2015.

supply chains in the Northeast. In addition, the problems at the terminal had a considerable impact on the operations of other terminals at the port.[36,37]

In addition to software errors having the potential to disrupt operations, malicious actors can exploit software flaws to gain access to maritime networks. Such flaws can include software vulnerabilities that have not been previously identified—"zero day" exploits—and known vulnerabilities that have not been appropriately mitigated through software patches.

NETWORK CONNECTIVITY AND INTERDEPENDENCIES

Many modern ICSs are Internet Protocol (IP) addressable and increasingly connected to company enterprise systems.[38] This not only increases connectivity and interoperability with other information systems, but also increases the exposure of ICSs to malicious actors. ICS interconnectivity can be seen in other networks used within seaports. Publicly available search engines, such as Shodan, can discover Internet-connected devices and be used by malicious actors to gain awareness of common devices used throughout maritime ICS.[39]

Mobile devices—including laptops, smartphones, and tablets—are often integrated into port networks. This includes personal laptops and other personal mobile devices.[40] The use of these products increases the number of potential entry points into a network for malicious actors.

Wireless networks are often used at ports to increase efficiency in operations and connectivity among platforms. If these networks are not properly secured and encrypted, they are vulnerable to penetration by malicious actors. In addition, open Wi-Fi is often offered as a service to crews of visiting vessels.

Operations at ports and aboard ships rely on more than one system. Failure of any one of these systems can produce cascading impacts in other systems and amplify the disruption to operations.[41] For example, ships rely heavily on GPS for navigation, whereas ports rely on GPS for cargo tracking and control.[42]

SOFTWARE SIMILARITIES

Ports and terminals across the globe often use similar software to load, unload, and track cargo. Vessels use the same software as many shipping companies. Because of the common software used by ships, ports, terminals, and shipping companies, multiple seaport facets could have consequences from malicious cyber activity. Software used by numerous ports or vessels, if vulnerable to exploitation by malicious actors, exposes other facilities to identical vulnerabilities and potential cyber attack vectors.

- ECDIS, usually installed on a vessel's bridge for navigation, is generally linked with many other onboard systems. Penetration testers and security firms have found numerous vulnerabilities inside ECDIS that would allow the software to be penetrated and manipulated, either directly or through other systems.[43,44]

---

[36] Mann, Ted, "Computer Problems Leave Goods Stranded at New York Port," The Wall Street Journal, August 4, 2013, www.wsj.com/articles/SB10001424127887323420604578648190833108164, accessed 9 October 2015.
[37] Bloomberg News, "New Jersey port gridlock eases as cargo computer system modified," August 5, 2013, www.nj.com/business/index.ssf/2013/08/new_jersey_port_gridlock_eases.html, accessed 9 October 2015.
[38] Ibid.
[39] For more information on Shodan, see O'Harrow Jr., Robert, "Cyber search engine Shodan exposes industrial control systems to new risks," the Washington Post, June 3, 2012, www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html, accessed 2 October 2015.
[40] Commander Joseph Kramek (USCG), "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities," The Brookings Institution, July 2013, www.brookings.edu/~/media/research/files/papers/2013/07/02%20cyber%20port%20security%20kramek/03%20cyber%20port%20security%20kramek.pdf, accessed 14 September 2015.
[41] John A. Volpe National Transportation Systems Center, "ICS Security in Maritime Transportation," Department of Transportation, July 2013, http://ntl.bts.gov/lib/48000/48000/48074/DOT-VNTSC-MARAD-13-01.pdfm, accessed 14 September 2015.
[42] Vice Admiral Charles D. Michel (USCG), Rear Admiral Paul F. Thomas (USCG), and Captain Andrew E. Tucci (USCG), "Cyber Risks in the Marine Transportation System," www.uscg.mil/hq/cg5/cg544/docs/USCG_Paper_MTS_CyberRisks.pdf, accessed 15 September 2015.
[43] Rouzer, Brett, "Cybersecurity and the Marine Transportation System," USCG Cyber Command, September 2015.
[44] Dyryavyy, Yevgen, "Preparing for Cyber Battleships–Electronic Chart Display and Information System Security," NCC Group, 2014, www.nccgroup.com/media/481230/2014-03-03_-_ncc_group_-_whitepaper_-_cyber_battle_ship_v1-0.pdf, accessed 10 September 2014.

FOREIGN DEPENDENCIES

Foreign hardware and software used by U.S. ports are vulnerable to the installation of malware during the manufacturing process. The act of installing foreign-manufactured hardware or software could be enough to compromise port networks.

- Between 2013 and 2014, malware dubbed "Zombie Zero" was preinstalled and hidden within Chinese-made scanner hardware used by shipping and logistic firms. The malware compromised at least eight companies. Once the scanner was plugged into a company's network, the malware compromised the network, established a remote connection to a location in China, and extracted financial and shipping information. Once inside the network, the malicious actors had complete visibility of financial data and the ability to modify shipping databases. The company that discovered the malware believes that it may have been the work of state actors.[45,46,47]

After the manufacturing process, software can remain vulnerable to malware installation by foreign actors during software updates.

GPS JAMMING AND SPOOFING

GPS spoofing devices attempt to deceive GPS receivers with signals resembling normal GPS signals; in contrast, jamming devices intentionally block or interfere with normal GPS signals. Exercises involving both methods could influence the operations of maritime vessels.

- In July 2013, researchers from the University of Texas at Austin took control of the navigational systems of a 210-foot yacht using only $3,000. The University of Texas group used a GPS spoofing device and injected its own signals into the vessel's GPS antennas, enabling it to steer the vessel as it saw fit. The onboard GPS did not indicate any of the changes in direction to the crew.[48,49]
- In 2008, the General Lighthouse Authorities of the United Kingdom (UK) and Ireland and the UK Ministry of Defence conducted a test in which a vessel sailed into a patch of ocean targeted by GPS jamming equipment.[50,51] Alarms activated for 10 minutes because different systems used to acquire and calculate the ship's position failed. The test included functionality of the differential GPS receivers, the automatic identification system transponder, the dynamic positioning system, the gyro calibration system, and the digital selective calling system. In addition, during the test, the ECDIS could not update and became a static screen. The vessel crew was able to navigate safely and prepare radar for parallel plotting. However, other ships would be unlikely to respond as quickly and smoothly, because the vessel crew had been prepared for the GPS-enabled equipment to fail.[52]

In addition to intentional disruptions of GPS signals at ports, unintentional GPS jamming at critical infrastructure facilities can result from persons using GPS jammers for other reasons.

- On August 4, 2012, the Newark Liberty International Airport experienced interference in its satellite-based plane tracking system because a pickup truck was carrying and operating a GPS jamming

---

[45] Lemos, Robert, "'Zombie Zero' Cyber-Attacks Hit Logistics, Robotic Firms for Months," eWeek, July 21, 2014, www.eweek.com/security/zombie-zero-cyber-attacks-hit-logistics-robotic-firms-for-months.html, accessed 15 September 2015.
[46] Cyberkeel, "Maritime Cyber-Risks," October 15, 2014, www.cyberkeel.com/images/pdf-files/Whitepaper.pdf, accessed 8 September 2015.
[47] TrapX Security, "TrapX Discovers 'Zombie Zero' Advanced Persistent Malware," July 10, 2014, http://trapx.com/07-09-14-press-release-trapx-discovers-zombie-zero-advanced-persistent-malware/, accessed 11 September 2015.
[48] UT Austin Cockrell School of Engineering, "UT Austin Researchers Spoof Superyacht at Sea," July 29, 2013, www.engr.utexas.edu/features/superyacht-gps-spoofing, accessed 8 September 2015.
[49] Cyberkeel, "Maritime Cyber-Risks," October 15, 2014, www.cyberkeel.com/images/pdf-files/Whitepaper.pdf, accessed 8 September 2015.
[50] Ibid.
[51] Grant, Alan, Williams, Paul, Ward, Nick and Sally Basker, "GPS Jamming and the Impact on Maritime Navigation," The General Lighthouse Authorities of the United Kingdom and Ireland, www.navnin.nl/NIN/Downloads/GLAs%20-%20GPS%20Jamming%20and%20the%20Impact%20on%20Maritime%20Navigation.pdf, accessed 10 September 2015.
[52] Parallel indexing involves creating a line parallel to the ship's desired course with a fixed perpendicular distance between the plotted course and the parallel line. The fixed distance between the lines allows a ship to keep track of any deviation from a planned course and helps keep a ship a safe distance from navigational dangers.

device. The employee claimed that he had the GPS jamming device in his truck to block the GPS his employer had installed in the vehicle.[53]

INSIDER THREATS

In a 2008 study, the National Infrastructure Advisory Council defined an insider threat to critical infrastructure as "one or more individuals with the access and/or insider knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with intent to cause harm."[54] A variety of factors, including greed, financial gain, anger at employer or dissatisfaction at work, blackmail, ideology or split loyalty, and ego can motivate these individuals.[55] Motivation and access to sensitive systems present an acute vulnerability in many critical infrastructure sectors, including the Maritime Subsector.

Intent to do harm is not required for insider threats to exist; careless and poorly trained individuals also represent a significant vulnerability in the operation of maritime networks.[56,57] These individuals can allow malicious actors into sensitive systems through several methods: executing malware sent through emails (phishing attack), accessing Websites that infect the computer with malware (watering hole attack), and manipulating them into providing sensitive information (social engineering).

POTENTIAL THREAT ACTIONS

A cyber attack by malicious actors on networks at a port or aboard a ship could result in lost cargo, port delays or disruptions, and physical and environmental damage, depending on the systems affected. The impact to port operations, which could last for days or weeks, depends on the damage done to port networks and facilities.

PORT OPERATIONS

DISRUPTION OF CARGO OPERATIONS

A malicious actor who gains access to terminal operating systems and cargo databases could erase, alter, or deny access to cargo-tracking software. Malicious actors have previously gained access to container tracking systems.

- Between 2011 and 2013, an organized crime group recruited hackers to breach IT systems that controlled the movement and location of containers at the Port of Antwerp, Belgium. Hackers first gained access by sending malware to port staff. After the initial breach was discovered and mitigated, hackers broke into port premises and attached key-logging devices onto computers. The group hid narcotics among legitimate cargo, and access to IT systems gave them the location and security details of containers, so they could send in drivers to steal the cargo before the legitimate owner arrived.[58,59]
- In 2012, crime syndicates penetrated the cargo systems used by Australian Customs and Border Protection, allowing them to see if their shipping containers were being regarded as suspicious by authorities. At least one private cargo tracking program relied on the data provided by Australian Customs and Border Protection, which could be accessed by the criminals.[60,61]

---

[53] Strunsky, Steve, "N.J. man fined $32k for illegal GPS device that disrupted Newark airport system," NJ.com, August 8, 2013, www.nj.com/news/index.ssf/2013/08/man_fined_32000_for_blocking_newark_airport_tracking_system.html, accessed 9 October 2015.
[54] Noonan, Thomas and Edmund Archuleta, "The Insider Threat to Critical Infrastructures," National Infrastructure Advisory Council, April 8, 2008, www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf, accessed 15 September 2015.
[55] Smith, Greg, "Combating Insider Threat," Proceedings of the Marine Safety & Security Council, Volume 71, Number 4, pp. 69–71, www.uscg.mil/proceedings/archive/2014/Vol71_No4_Wint2014.pdf, accessed 14 September 2015.
[56] Government Accountability Office, "Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity," June 2014, www.gao.gov/assets/670/663828.pdf, accessed 14 September 2015.
[57] Colonel Steve Coppinger (USAF, Ret.), "The Frenemy: Insider Threats in the Maritime Environment," Proceedings of the Marine Safety & Security Council, Volume 71, Number 4, pp. 77–80, www.uscg.mil/proceedings/archive/2014/Vol71_No4_Wint2014.pdf, accessed 14 September 2015.
[58] Bateman, Tom, "Police warning after drug traffickers' cyber-attack," BBC, October 16, 2013, www.bbc.com/news/world-europe-24539417, accessed 8 September2015.
[59] Robertson, Jordan and Michael Riley, "The Mob's IT Department," Bloomberg Businessweek, July 7, 2015, www.bloomberg.com/graphics/2015-mob-technology-consultants-help-drug-traffickers/, accessed 8 September 2015.
[60] Cyberkeel, "Maritime Cyber-Risks," October 15, 2014, www.cyberkeel.com/images/pdf-files/Whitepaper.pdf, accessed 8 September 2015.

In a worst-case scenario, the denial or loss of cargo information could bring port operations to a complete halt. U.S. seaports, for example, can hold thousands of containers at one time. If backup is unavailable for cargo information, identifying and locating containers and the cargo inside could take weeks, and the capability of the port to receive and distribute cargo could be significantly hampered.

- In 2011, the state-owned Islamic Republic of Iran Shipping Lines was the victim of a cyber attack that crashed its system and resulted in the loss of all data tracking its carriers, including data related to rates, loading, cargo number, date, and place. The location for all shipping containers was unknown. This led to significant disruption in operations, financial losses, and lost cargo.[62,63]

ACCESSING ICS

Malicious actors could disrupt ICSs used within a port, including the systems used to control gantry cranes and bulk cargo handling systems. Without these ICSs, ships cannot be loaded and unloaded, resulting in a disruption of port operations until ICSs are restored.

Access to ICSs within a port could allow a malicious actor to cause significant physical damage to port facilities. For example, access to the ICS controlling automated gantry cranes could damage the cranes, which in turn could have a significant impact on container operations at a port. Another example is manipulation of valves and critical safety systems in a fuel transfer that could result in an explosion and the release of pollutants into waterways.[64] Such an attack could result in a disruption at the port for weeks or months.

Attacks resulting in physical damage can initially appear as mechanical or human failure, and it could take weeks to connect the incident to a cyber vulnerability.[65] Until a cyber vulnerability is identified and mitigated, malicious actors can continue exploiting the ICS.

GPS DISRUPTION

Some equipment within ports, such as automated gantry cranes, relies on GPS to operate effectively. A disruption in their ability to use GPS—whether through equipment manipulation or the intentional or unintentional blocking of GPS signals—can effectively deny the usage of this equipment and disrupt port operations until GPS capability is restored.

- A GPS anomaly at a U.S. port in 2013 affected four automated cranes for more than 7 hours. Disruption of the GPS signal caused two cranes to stop working and degraded the operability of two additional cranes.[66]

OTHER MALICIOUS ACTIVITIES

The capability to manipulate access control and monitoring systems—even with no direct effect to cargo movement—would allow malicious actors to enter ports with less difficulty. Malicious actors could, for example, use this access to manipulate video surveillance feeds and steal the credentialing information of those with access to the port. This could be used to facilitate other malicious activities, including criminal and terrorist acts.

The interruption to business operation networks, such as those used for billing and communications, could also disrupt operations at a terminal or port. The terminal operator(s) would have diminished capacity to function effectively until these systems are restored.

---

[61] Kochetkova, "Maritime industry is easy meat for cyber criminals," Kaspersky Labs, May 22, 2015, https://blog.kaspersky.com/maritime-cyber-security/8796/, accessed 8 September 2015.
[62] Cyberkeel, "Maritime Cyber-Risks," October 15, 2014, www.cyberkeel.com/images/pdf-files/Whitepaper.pdf, accessed 8 September 2015.
[63] Hutchins, Reynolds, "Carriers threatened by cyber attacks, experts warn," Journal of Commerce, March 3, 2015, www.joc.com/maritime-news/container-lines/carriers-threatened-cyber-attacks-experts-warn_20150303.html, accessed 8 September 2015.
[64] LCDR Jennifer Konon, "Control System Cybersecurity," Proceedings of the Marine Safety & Security Council, Volume 71, Number 4, pp. 45–47, www.uscg.mil/proceedings/archive/2014/Vol71_No4_Wint2014.pdf, accessed 2 September 2015.
[65] John A. Volpe National Transportation Systems Center, "ICS Security in Maritime Transportation," Department of Transportation, July 2013, http://ntl.bts.gov/lib/48000/48000/48074/DOT-VNTSC-MARAD-13-01.pdf, accessed 14 September 2015.
[66] Rouzer, Brett, "Maritime Cyber Security Standards Public Meeting," Guidance on Maritime Cyber Security Public Meeting, January 15, 2015, 48:50, www.youtube.com/watch?v=rzOVc1ZOuvY#t=2975, accessed 11 September 2015.

In addition to manipulating access control and monitoring systems, malicious actors could use cyber activities to divert attention from other undertakings, including other cyber actions. For example, distributed denial of service attacks have been used to divert attention from other security incidents, including data-theft and network-damaging attempts.[67]

SHIP OPERATIONS

GPS JAMMING AND SPOOFING

When close to a port, tugboats and pilots assist in moving oceangoing vessels making it less likely that GPS jamming or spoofing will have a significant impact. However, when a tugboat and pilot are not used, or when a vessel is not otherwise under physical control of the vessel crew, and visual navigation aids are not being closely monitored, GPS jamming or spoofing can significantly affect the movement of a ship.

GPS jamming or spoofing can cause a ship to veer off course possibly becoming grounded or collide with another vessel, especially when operating within a narrow shipping channel. The consequence of such an event could be major for a vessel carrying hazardous cargo. A grounded or damaged ship can close a port or shipping channel for days and affect or halt operations at ports upstream; however, the delay is unlikely to be long enough to have a significant impact on operations.

The greatest risk is collision due to a ship with hazardous cargo that has sunk in a shipping channel. Such an event could close down a shipping channel for weeks, which could have a significant impact on port terminals upstream of the incident.

An ECDIS is usually interconnected with other sensors and systems on a ship. It is often connected to the Internet through the shipboard network where security weaknesses have the potential to be exploited. Malicious actors can subvert sensor data and misrepresent it to a ship's ECDIS, which can influence the navigation by ship personnel and increase the risk of a ship running aground or colliding with another ship.[68,69]

- On January 17, 2013, the USS *Guardian,* an *Avenger* class mine countermeasure ship, ran aground on Tubbataha Reef in the Sulu Sea in the Philippines. According to an investigation completed by the U.S. Navy, *Guardian* crew relied on inaccurate digital nautical charts during the planning and execution of the navigation plan; thus, the watch team disregarded visual cues, electronic cues, and alarms leading up to the grounding.[70] The U.S. Navy ultimately decided to scrap the $277 million vessel.[71]

ICS ACCESS

A malicious actor could shut down a ship by either taking control of certain onboard ICS or damaging ICS directly. When in port, this could prevent a ship from departing, resulting in delays at the terminal where the ship is located. If disabled while underway, the vessel could block shipping channels or present a hazard to other ships in the area.

The potential for malicious actors to manipulate the engine ICS poses a significant risk. Malicious actors could manipulate engine controls to damage the engine or prompt a fire or explosion that could be a significant danger to the ship. Through manipulating ICS, engine controls could increase or decrease the speed of a vessel. Although onboard crew would likely notice a change in speed, such an action in a narrow shipping channel or close to a port poses a significant risk of a larger vessel running aground or colliding with other vessels.

---

[67] Greene, Tim, "Under DDoS attack? It could be just a distraction," Network World, September 17, 2015, www.computerworld.com/article/2984606/security/under-ddos-attack-it-could-be-just-a-distraction.html, accessed 21 September 2015.
[68] Rouzer, Brett, "Cybersecurity and the Marine Transportation System," USCG Cyber Command, September 2015.
[69] Dyryavyy, Yevgen, "Preparing for Cyber Battleships–Electronic Chart Display and Information System Security," NCC Group, 2014, www.nccgroup.com/media/481230/2014-03-03_-_ncc_group_-_whitepaper_-_cyber_battle_ship_v1-0.pdf, accessed 10 September 2014.
[70] U.S. Pacific Fleet Public Affairs, "USS Guardian Grounding Investigation Results Released," June 20, 2013, www.navy.mil/submit/display.asp?story_id=74930, accessed 14 September 2015.
[71] Whaley, Floyd, "U.S. Navy to Scrap Vessel Stuck on Philippine Reef," New York Times, January 31, 2013, www.nytimes.com/2013/02/01/world/asia/us-navy-to-scrap-vessel-stuck-on-philippine-reef.html, accessed 14 September 2015.

Access to ICS allows malicious actors to manipulate or disable other onboard sensors and alarms. This could affect a variety of systems, including fire suppression, navigation sensors, bilge pumps, and engine alarms. Disabling or manipulating these sensors and alarms could result in significant damage to a vessel, especially if combined with other malicious activities.

EFFECTS TO CRITICAL INFRASTRUCTURE

The impact to critical infrastructure sectors depends on the port affected by a cyber attack, the level and length of disruption that occurs at the port, and the capability to divert shipments to other ports. Although all Sectors rely to some degree on the goods that transit U.S. ports, those most likely to be affected by a disruption are Critical Manufacturing, Commercial Facilities, Food and Agriculture, Energy, Chemical, and Transportation Systems. A greater impact to critical infrastructure is likely if more than one port is disrupted by a cyber attack.

CRITICAL MANUFACTURING

Many industries within the Critical Manufacturing Sector rely upon "just-in-time" supply chains that could be disrupted if the import of material necessary for manufacturing were delayed by an interruption of port operations. Depending on the location and duration of port disruptions, companies within the Critical Manufacturing Sector could be forced to reduce or halt production of certain products until port operations return to normal or apply another method of importation outside of the affected ports.

- During the 2014–15 labor slowdown at West Coast ports, Honda North America, Incorporated, reduced production at factories in Ohio and Indiana because crucial auto parts from Japan could not be imported.[72]
- In 2002, five car factories shut down during the closure of West Coast ports because of supply chain disruptions.[73]

Many industries depend on the Critical Manufacturing Sector to provide the materials and products necessary to perform their own essential functions. This includes segments of the Critical Manufacturing Sector relying on other segments within the Sector for components and finished products. A disruption within one segment of the Critical Manufacturing Sector could cause a cascading impact on other industries both inside and outside of the Sector.

COMMERCIAL FACILITIES

Like the Critical Manufacturing Sector, many businesses within the Commercial Facilities Sector rely heavily on just-in-time supply chains. Because of the limited inventory levels associated with these supply chains, a disruption at a port could negatively affect businesses in the Sector whose supply chains are interrupted.

- A retail-consulting firm projected that the 2014–15 West Coast ports slowdown would cost the retail industry $7 billion in 2015. The loss was due to missed sales, below optimal inventory levels, and the higher price of moving goods during the slowdown.[74,75]
- In October 2012, Hurricane Sandy affected all operations at the Port of New York and New Jersey, the largest port on the East Coast. Areas of the Port closed for 3–5 days.[76] Rail service to and from the port was significantly affected, leading to additional delays. The port closure and delays had a significant impact on supply chains in the Commercial Facilities Sector resulting in shipping delays and lower than normal inventories for many retail companies along the East Coast.[77,78]

---

[72] Khouri, Andrew, "Q&A Port dispute: What you need to know," Los Angeles Times, February 25, 2015, www.latimes.com/business/la-fi-port-dispute-qa-20150212-story.html, accessed 13 August 2015.
[73] The Economist, "Dock Around the Clock," November 28, 2002, www.economist.com/node/1468299, accessed 13 August 2015.
[74] Reagan, Courtney, "West Coast ports: Retail's $7 billion problem," CNBC, February 9, 2015, www.cnbc.com/2015/02/09/west-coast-ports-retails-7-billion-problem.html, accessed 13 August 2015.
[75] Halzack, Sarah, "Why a major backup at West Coast ports could cost the retail industry billions," the Washington Post, February 17, 2015, www.washingtonpost.com/news/wonkblog/wp/2015/02/17/why-a-major-backup-at-west-coast-ports-could-cost-the-retail-industry-billions/, accessed 13 August 2015.
[76] Commander Linda A. Sturgis (USCG), Smyth, Tiffany, and Captain Andrew E. Tucci (USCG), "Port Recovery in the Aftermath of Hurricane Sandy," Center for a New American Security, August 2014, www.cnas.org/sites/default/files/publications-pdf/CNAS_HurricaneSandy_VoicesFromTheField.pdf, accessed 8 October 2015.
[77] Clifford, Stephanie and Nelson Schwartz, "A Storm-Battered Supply Chain Threatens Holiday Shopping," The New York Times, November 4, 2012, www.nytimes.com/2012/11/05/business/a-storm-battered-supply-chain-threatens-the-holiday-shopping-season.html?_r=0, accessed 8 October 2015.

FOOD AND AGRICULTURE

In 2013, 75 percent of U.S. agricultural exports (128 million metric tons) and 70 percent of imports (42 million metric tons) were waterborne. Of the 128 million metric tons exported, 28 percent moved in containers. Three Louisiana ports—New Orleans, South Louisiana, and Baton Rouge—accounted for 40 percent of waterborne agricultural exports by total metric tons (Figure 3), and five West Coast ports—Los Angeles, Long Beach, Oakland, Tacoma, and Seattle—were the largest for containerized exports. About 69 percent of all waterborne imports moved in containers. The largest U.S. ports for bulk and containerized agricultural imports were New York, Los Angeles, Philadelphia, Oakland, and Houston.[79]

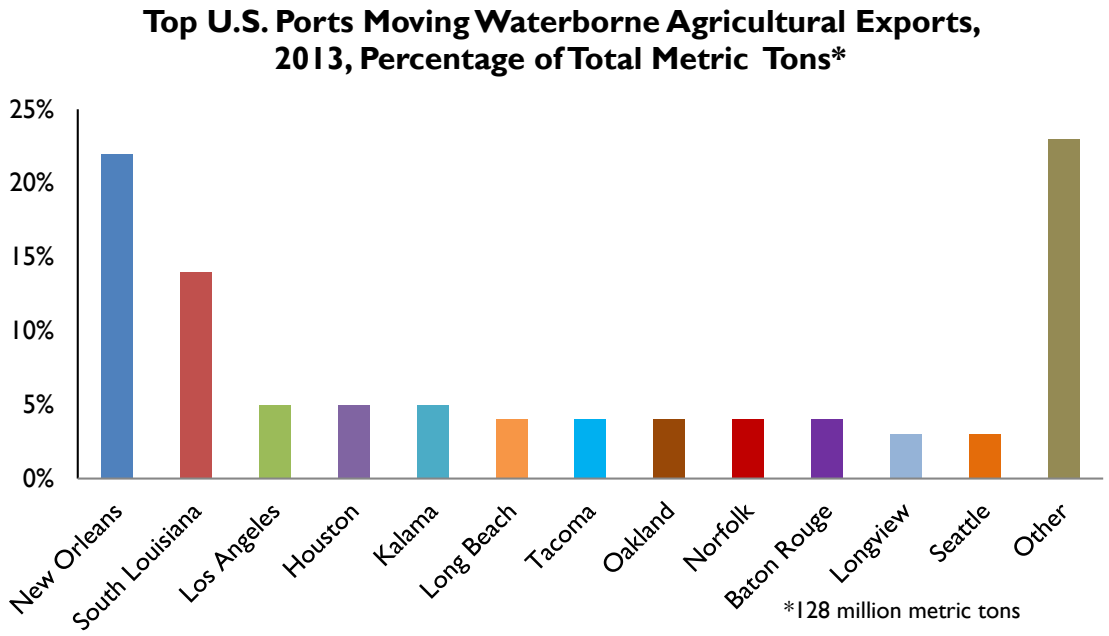

FIGURE 3—WATERBORNE AGRICULTURAL EXPORTS BY PORT AS PERCENTAGE OF TOTAL METRIC TONS[80]

Delays in the movement of perishable goods can increase the amount of product that spoils and lead to higher transportation costs and decreasing revenues for businesses in the Food and Agriculture Sector. Producers may instead increase the amount of product sold in domestic markets, which can decrease prices and revenues for other producers who focus on the domestic market.

- During the 2014–15 West Coast ports slowdown, food products spoiled at an increased rate because of increased waiting time for shipping. Accordingly, Tyson Foods, the largest meat processor in the United States, had to redirect its beef sales at lower prices.[81,82]

Horticultural products, sugar, and tropical products account for more than 61 percent of all U.S. agricultural imports. A disruption of operations at ports that focuses on agricultural imports could result in lower inventories and potential shortages of some of these products.[83,84,85]

---

[78] Strategic Sourceror, "After Sandy, retail logistics a challenge," November 7, 2012, www.strategicsourceror.com/2012/11/after-sandy-retail-logistics-challenge.html, accessed 8 October 2015.
[79] USDA, "A Reliable Waterway System Is Important to Agriculture," October 2014, www.ams.usda.gov/sites/default/files/media/Importance%20of%20Waterways%2010-2014.pdf, accessed 22 September 2015.
[80] Ibid.
[81] White, Martha, "West Coast Port Labor Gridlock Makes Agricultural Exports Suffer," NBC News, February 13, 2015, www.nbcnews.com/business/business-news/west-coast-port-labor-gridlock-makes-agricultural-exports-suffer-n305806, accessed 13 August 2015.
[82] Bonney, Joseph, "West Coast woes forced Tyson to discount beef exports," Journal of Commerce, August 6, 2015, www.joc.com/port-news/longshoreman-labor/international-longshore-and-warehouse-union/west-coast-woes-forced-tyson-sell-beef-exports-less_20150806.html, accessed 13 August 2015.
[83] Horticultural products include fruits, vegetables, tree nuts, wine, essential oils, nursery stock, cut flowers, and hops.
[84] Sugar and tropical products include sugar, coffee, cocoa, and rubber.

ENERGY

Although a significant increase in domestic crude oil production has occurred during the past several years, imports still account for 27 percent of petroleum consumed in the United States.[86] In 2014, maritime shipping accounted for 5.1 million barrels of petroleum products per day via ship, representing 55 percent of all U.S. daily petroleum imports. .[87,88] Regions of the United States still heavily depend on foreign sources of crude oil.

- California depends on foreign oil imports and refines it in-state because of its geographic distance from other oil-producing regions; California has more than 10 percent of U.S. refining capacity.[89] In 2014, more than 51 percent of oil supplied to California refineries came from foreign sources, roughly 37 percent came from California sources, and 10 percent came from Alaska (Figure 4).[90] The largest foreign suppliers of crude oil were Saudi Arabia (35.51 percent of foreign sources), Iraq (21 percent), Ecuador (17.1 percent), and Colombia (8.7 percent).[91,92] The vast majority of crude from Alaska and foreign sources is transported by ship and received at ports in Los Angeles, Long Beach, and the Bay Area. The relative isolation of California, along with the specific requirements and regulations of the State's fuel markets, makes the price of petroleum products in California more volatile.[93]

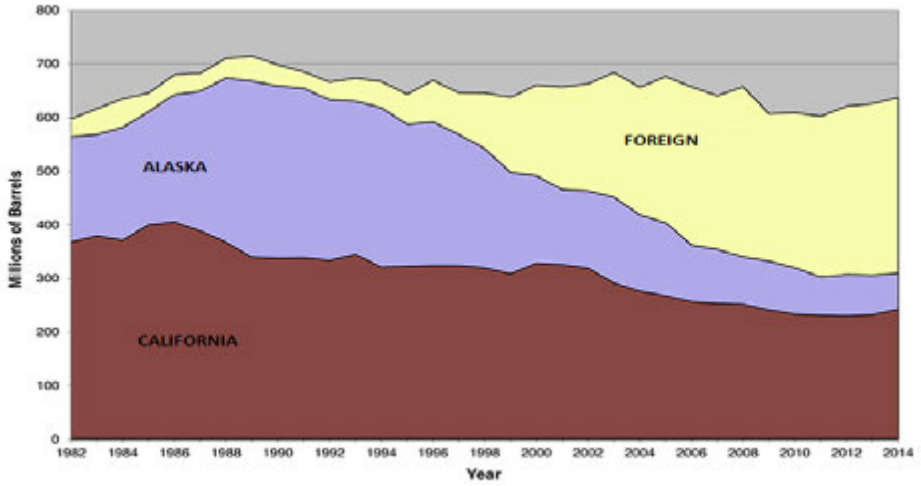

FIGURE 4—CRUDE OIL SUPPLY SOURCES TO CALIFORNIA REFINERIES[94]

A malicious cyber incident that disrupted the import of crude oil could temporarily increase the volatility in the price of gasoline and other petroleum-derived products within a region. Potential regional shortages would depend on how quickly import operations could be restored and the capability to transport crude oil and finished petroleum products from elsewhere.

- Gasoline prices in California also increased following the February 18, 2015, explosion at an ExxonMobil refinery in Torrance, California, increasing 25 cents in less than a week and increasing another 25 cents as

[85] USDA Economic Research Service, "Close to two-thirds of U.S. agricultural imports consist of horticultural and tropical products," www.ers.usda.gov/data-products/chart-gallery/detail.aspx?chartId=40090&ref=collection&embed=True&widgetId=39734, accessed 22 September 2015.
[86] EIA, "How much petroleum does the United States import and from where?," last updated September 14, 2015, www.eia.gov/tools/faqs/faq.cfm?id=727&t=6, accessed 23 September 2015.
[87] Petroleum includes crude oil, refined petroleum products such as gasoline and diesel fuel, biofuels, chemical feedstocks, and other petroleum products.
[88] EIA, "Imports by Area of Entry," updated August 31, 2015, www.eia.gov/dnav/pet/pet_move_imp_dc_NUS-Z00_mbbl_a.htm, accessed 17 September 2015.
[89] Energy Information Administration, "California State Profile and Energy Estimates," last updated June 16, 2014, www.eia.gov/state/analysis.cfm?sid=CA, accessed 20 April 2015.
[90] According to the California Energy Commission, the California crude total also includes minor amounts from North Dakota and the Gulf Coast states.
[91] California Energy Commission, "Oil Supply Sources to California Refineries," http://energyalmanac.ca.gov/petroleum/statistics/crude_oil_receipts.html, accessed 22 September 2015.
[92] California Energy Commission, "Foreign Sources of Crude Oil Imports to California 2014," http://energyalmanac.ca.gov/petroleum/statistics/2014_foreign_crude_sources.html, accessed 22 September 2015.
[93] EIA, "California: Profile Analysis," last updated September 17, 2015, www.eia.gov/state/analysis.cfm?sid=CA, accessed 28 September 2015.
[94] California Energy Commission, "Oil Supply Sources to California Refineries," http://energyalmanac.ca.gov/petroleum/statistics/crude_oil_receipts.html, accessed 22 September 2015.

of March 9.[95,96] Although these incidents involved a lowering of refinery capacity, an event that affects the import of crude oil could have a similar or greater effect on the price of petroleum products in California.

- Following the August 6, 2012, fire at the Chevron refinery in Richmond, California, gasoline prices in California increased more than 25 cents in the week following the fire. Gas prices hit a high of $4.707 per gallon in October (2 months after the fire)—a $0.79 increase—before returning to pre-fire prices in November.[97,98]

Petroleum Administration for Defense District 3, which includes the states along the Gulf Coast, is an important supplier of gasoline for the Gulf Coast, Midwest, and East Coast. Petroleum Administration for Defense District 3 was the point of entry for more than 40 percent of all crude oil and petroleum product imports in the United States in 2014.[99,100] More than 35 percent of all 2013 vessel calls by tankers at U.S. ports occurred at two Gulf Coast ports: the Sabine-Neches Waterway and the Port of Houston.[101] An incident in the shipping lanes at either port can have an impact on refineries upstream.

- On March 9, 2015, the Liberian-flagged bulk carrier *Conti Peridot* and the Danish-flagged *Carla Maersk* collided in foggy conditions in the Houston Ship Channel. The *Carla Maersk* was significantly damaged with a rupture in two cargo tanks carrying the flammable compound methyl tertiary butyl ether. The Houston Ship Channel was closed for 3 days while the spill was cleaned up and the ship was repaired.[102,103,104] The section of the port that was closed leads to five refineries with 1.34 million barrels per day (bpd) of capacity, representing more than 7 percent of U.S. refining capacity.[105,106] Based on the March 9 incident, ExxonMobil cut production at its 560,500 bpd refinery in Baytown, Texas.[107] The Baytown refinery is the second largest refinery in the United States.[108]

An incident that disrupts port operations at either of these locations for several days or weeks, such as the sinking of a vessel in one of the deep-draft shipping lanes, could have a significant impact on the price of petroleum products regionally and nationally.

Malicious cyber actors could also disrupt the export of certain energy products. For example, a disruption at the seaport in Norfolk, Virginia, would disrupt the facilities responsible for approximately 40 percent of U.S. coal exports from 2000–2010.[109]

---

[95] Flaccus, Gillian, "Gas prices soar in California as supply shrinks," The Associated Press, 2/27/2015, http://www.sacbee.com/news/business/article11389799.html, accessed 12 March 2015.
[96] Energy Information Administration, "Weekly California All Grades All Formulations Retail Gasoline Prices," http://www.eia.gov/dnav/pet/hist/LeafHandler.ashx?n=PET&s=EMM_EPM0_PTE_SCA_DPG&f=W, accessed 12 March 2015.
[97] Glover, Mark, "California's Gas Prices Soar After Chevron Refinery Fire," Sacramento Bee, August 14, 2012, www.sacbee.com/2012/08/14/4723764/californias-gas-prices-soar-after.html, accessed 12 March 2012.
[98] Energy Information Administration, "Weekly California All Grades All Formulations Retail Gasoline Prices," http://www.eia.gov/dnav/pet/hist/LeafHandler.ashx?n=PET&s=EMM_EPM0_PTE_SCA_DPG&f=W, accessed 12 March 2015.
[99] Energy Information Administration, "U.S. Imports of Crude Oil and Petroleum Products," September 30, 2015, www.eia.gov/dnav/pet/hist/LeafHandler.ashx?n=pet&s=mttimp31&f=a, accessed 6 October 2015.
[100] Energy Information Administration, "Gulf Coast (PADD 3) Imports of Crude Oil and Petroleum Products," September 30, 2015, www.eia.gov/dnav/pet/hist/LeafHandler.ashx?n=pet&s=mttimp31&f=a, accessed 6 October 2015.
[101] Maritime Administration, "2013 Vessel Calls in U.S. Ports and Terminal Privately-owned, oceangoing merchant vessels over 1,000 gross tons," U.S. Department of Transportation, www.marad.dot.gov/wp-content/uploads/xlsx/DS_U.S.-Port-Calls-2013.xlsx, accessed 6 October 2015.
[102] KHOU-TV (Houston, TX), "Tanker, bulk carrier collide in Houston Ship Channel," March 9, 2015, www.usatoday.com/story/news/nation/2015/03/09/ships-collide-in-houston-ship-channel/24679025/, accessed 23 September 2015.
[103] Horansky, Andrew, "Houston Ship Channel remains closed after collision," KHOU-TV (Houston, TX), March 11, 2015, www.usatoday.com/story/news/nation/2015/03/11/houston-ship-channel-remains-closed-for-cleanup/70181692/, accessed 23 September 2015.
[104] Lezon, Dale, "Houston Ship Channel reopens after collision," Houston Chronicle, March 12, 2015, www.chron.com/news/houston-texas/article/Ship-Channel-reopens-6129873.php, accessed 23 September 2015.
[105] Weber, Harry and Dan Murtaugh, "Exxon Baytown Plant Cuts Rates With Channel Section Shut," Bloomberg, March 11, 2015, www.bloomberg.com/news/articles/2015-03-11/exxon-baytown-refinery-affected-by-ship-channel-section-shutdown, accessed 6 October 2015.
[106] Energy Information Administration, "Number and Capacity of Petroleum Refineries," June 19, 2015, www.eia.gov/dnav/pet/pet_pnp_cap1_dcu_nus_a.htm, accessed 6 October 2015.
[107] Weber, Harry and Dan Murtaugh, "Exxon Baytown Plant Cuts Rates With Channel Section Shut," Bloomberg, March 11, 2015, www.bloomberg.com/news/articles/2015-03-11/exxon-baytown-refinery-affected-by-ship-channel-section-shutdown, accessed 6 October 2015.
[108] Energy Information Administration, "Top 10 U.S. refineries operable capacity," July 10, 2015, www.eia.gov/energyexplained/index.cfm?page=oil_refining#tab4, accessed 6 October 2015.
[109] Energy Information Administration, "Six seaports account for 94% of U.S. coal exports, which are dominated by coking coal," November 8, 2011, www.eia.gov/todayinenergy/detail.cfm?id=3830, accessed 22 September 2015.

CHEMICAL

Ports play an important role in the import and export of various chemicals. In 2014, the United States imported more than $205 billion and exported more than $200 billion worth of chemicals, including pharmaceuticals. Except for Canada, the 10 largest chemical exporters to the United States are in Europe and Asia, including Ireland, Germany, China, Switzerland, and Japan.[110]

The effect of a port shutdown on the Chemical Sector depends on the ports affected, the chemicals transported through the ports, the available inventories, and the capability of businesses within the Chemical Sector to work around any affected chemical supply chains. A disruption in chemical import supply chains could result in a temporary increase of domestic prices for the affected chemicals. If one or more ports shut down or significantly reduce operations for days or weeks, companies both inside and outside of the Chemical Sector could experience a shortage of certain chemicals hampering production of manufactured chemicals and other goods.

- The 2015 West Coast ports labor dispute resulted in the delay of some chemical shipments. Impacts of the slowdown included increased container shipment rates and delayed shipments, some up to a month late.[111]

TRANSPORTATION SYSTEMS

If one or more ports become unable to accept or distribute cargo, the Maritime and Freight Rail Subsectors would be affected regionally. Such disruptions could result not only in rerouting of trains and barges, but also in overloading of ports that receive additional ships and cargo from those ports. More time, trains, and trucks would be needed to move that cargo through the port, which could result in significant congestion and delays.

Within the Aviation Subsector, air freight services could see a significant increase in cargo following a port disruption.[112] This increase could cause congestion within the logistic chains of air freight companies, leading to delays in the movement of goods.

In the Highway Infrastructure and Motor Carrier Subsector, an interruption of port operations could disrupt the logistic chains of trucking companies. This could lead to delays and significant economic impacts for the affected trucking companies. The Mass Transit and Passenger Rail Subsector is unlikely to experience any operational impacts due to a port disruption.

MITIGATION MEASURES

Several mitigation measures can increase the security and resiliency of ports: instituting maritime cybersecurity standards, sharing information across the sector, conducting routine vulnerability assessments, ensuring personnel use best practices, mitigating insider threats, and developing contingency plans for cyber attacks.

Cybersecurity standards can help maritime organizations address risks and enhance the resilience of critical networks within the Maritime Subsector. The 2014 National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity assists organizations in applying best practices of risk management to improve critical infrastructure security and resiliency.[113] In addition, the U.S. Coast Guard is evaluating cybersecurity standards for the Maritime Subsector. This effort is progressing at a measured pace to ensure that the public and private sectors and industry partners engage in the discussion for the way ahead.

---

[110] International Trade Administration, "Global Patterns of U.S. Merchandise Trade," Department of Commerce, http://tse.export.gov/TSE/TSEOptions.aspx?ReportID=1&Referrer=TSEReports.aspx&DataSource=NTD, accessed 21 September 2015.
[111] ICIS, "West coast port slowdowns disrupt some chemical markets," February 12, 2015, www.icis.com/resources/news/2015/02/12/9860754/west-coast-port-slowdowns-disrupt-some-chemical-markets/, accessed 21 September 2015.
[112] Hsu, Tiffany, "Air freight firms are bustling amid bottlenecks at West Coast ports," The Los Angeles Times, February 20, 2015, www.latimes.com/business/la-fi-air-cargo-20150221-story.html, accessed 8 October 2015.
[113] For more on the NIST framework, see: NIST, "Framework for Improving Critical Infrastructure Cybersecurity," February 12, 2014, www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, accessed 24 September 2015.

Information sharing is critical for ports to obtain information about vulnerabilities to maritime networks, effective mitigation measures, and other effective contingency and protection plans. Beneficial information sharing can occur among the government, private maritime partners, and other groups interested in the security and reliability of maritime networks.

In addition to cybersecurity standards, ports and other maritime industries can conduct vulnerability assessments and exercises. Assessments can allow organizations within the Maritime Subsector to identify and mitigate network vulnerabilities.[114,115] Regular use of vulnerability software and timely software and firmware patching can help prevent malicious actors from exploiting known vulnerabilities to launch cyber attacks.

Ensuring that personnel use best practices can lower the risk of malicious actors gaining access to maritime networks. These practices include cybersecurity training, strong passwords, awareness of phishing scams and suspect sites, and flash drive prohibition.[116] Taking steps to mitigate insider threats can lower the risk to maritime networks. These steps include understanding indicators of malicious threat activity, effective deterrence methods, and continual training.[117]

Measures can be taken to mitigate the impacts of a cyber attack. Manual backups can help mitigate the impacts of a network failure that disrupts port operations, providing that the network backup is reliable and personnel are trained in its use.[118] Having dedicated cyber incident response plans (including plans to isolate, test, and repair) for resuming operations of affected systems can allow a port to recover quickly from cyber attacks.[119]

Vessel operators can route ships to other ports, and companies can increase their use of other freight modes to mitigate some of the disruption caused by an interruption in port operations. These measures, however, are unlikely to mitigate all cargo disruptions due to limited capacity and increased expense. The use of other ports can increase shipping times and cause delays at other ports because of increased cargo traffic. In addition, the lack of advanced warning would also limit the ability to redirect shipments immediately following a disruption caused by malicious cyber activity.

The Office of Cyber and Infrastructure Analysis (OCIA) provides innovative analysis to support public and private-sector stakeholders' operational activities and effectiveness and inform key decisions affecting the security and resilience of the Nation's critical infrastructure. All OCIA products are visible to authorized users at HSIN-CI and Intelink. For more information, contact OCIA@hq.dhs.gov or visit http://www.dhs.gov/office-cyber-infrastructure-analysis.

[114] Vice Admiral Charles D. Michel (USCG), Rear Admiral Paul F. Thomas (USCG), and Captain Andrew E. Tucci (USCG), "Cyber Risks in the Marine Transportation System," www.uscg.mil/hq/cg5/cg544/docs/USCG_Paper_MTS_CyberRisks.pdf, accessed 15 September 2015.
[115] Commander Joseph Kramek (USCG), "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities," The Brookings Institution, July 2013, www.brookings.edu/~/media/research/files/papers/2013/07/02%20cyber%20port%20security%20kramek/03%20cyber%20port%20security%20kramek.pdf, accessed 2 September 2015.
[116] Tucci, Andrew, "Dial 'C' for Cyber Attack," Proceedings of the Marine Safety & Security Council, Volume 72, Number 2, pp. 48–51, http://uscgproceedings.epubxp.com/t/11313-proceedings-of-the-marine/50, accessed 24 September 2015.
[117] For more information, see: National Cybersecurity and Communications Integration Center, "Combating the Insider Threat," Department of Homeland Security, May 2, 2014, www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat.pdf, accessed 24 September 2015.
[118] Vice Admiral Charles D. Michel (USCG), Rear Admiral Paul F. Thomas (USCG), and Captain Andrew E. Tucci (USCG), "Cyber Risks in the Marine Transportation System," www.uscg.mil/hq/cg5/cg544/docs/USCG_Paper_MTS_CyberRisks.pdf, accessed 15 September 2015.
[119] Tucci, Andrew, "Dial 'C' for Cyber Attack," Proceedings of the Marine Safety & Security Council, Volume 72, Number 2, pp. 48–51, http://uscgproceedings.epubxp.com/t/11313-proceedings-of-the-marine/50, accessed 2 September 2015.