The Little-known Challenge of Maritime Cyber Security*

Joseph DiRenzo
Senior Advisor for Science, Technology, Innovation
US Coast Guard Atlantic Area
Norfolk, Virginia, USA
Joseph.DiRenzo@uscg.mil

Dana A. Goward
Resilient Navigation and Timing Foundation
Alexandria, Virginia, USA
dgoward@rntfnd.org

Fred S. Roberts
CCICADA Center
Rutgers University
Piscataway, New Jersey, USA
froberts@dimacs.rutgers.edu

Abstract – **The vulnerabilities to cyber attacks of today's marine transportation system have not been well studied. This paper explores vulnerabilities of shipboard systems, oil rigs, cargo, and port operations.**

Keywords: cyber security, shipboard systems, cargo handling, port operations, GPS jamming, electronic chart display and information system, automatic identification system

I. INTRODUCTION

Computer networks control some of the most important critical infrastructure in the world. This includes power systems, water supply systems, air traffic control, building control systems, and transportation systems. This infrastructure is vulnerable to failures of computer systems or deliberate cyber attacks, and the concern about such attacks has been widely discussed. What is not so well known are the specific vulnerabilities of today's marine transportation system to cyber attacks. The dependence of many maritime systems on the Global Positioning System (GPS), and the relative ease by which these systems can be jammed (through denial of reception by a competing signal) or spoofed (through deliberate introduction of a false signal) is of particular concern. GPS is a vital part of a broad array of shipboard, port, and even oil rig systems. Market forces and advances in technology are integrating these systems with one another, and with other systems, increasing both vulnerabilities and the potential consequences in the event of system failure. These vulnerabilities and potential countermeasures have not been well studied and, indeed, there have been almost no peer-reviewed articles on the topic of maritime cyber security.

The maritime transportation system (MTS) is critical to the world's economy. Indeed, a vast majority of goods in international trade are still transported by sea. Disruption of the global supply chain for commodities such as oil or food could cause dramatic problems for the world-wide economy. Disruption of the MTS could cause billions of dollars in damage to the economy. For the United States alone, "Oceans and seaports are gateways for economic growth, opportunity, and prosperity. America's economic strength is dependent on freedom of the seas as well as an efficient system of ports and waterways for commercial movement of people, cargo, and conveyances" [1]. During the month of January 2015, the ports on the West Coast of the United States were closed due to a labor stoppage and the impact on the economy was dramatic [2].

II. SHIPBOARD SYSTEMS

A 2013 demonstration by a research team at the University of Texas–Austin showed how a potential adversary could remotely take control of a vessel by manipulating its Global Positioning System (GPS). The yacht "White Rose of Drax" was successfully "spoofed" while sailing on the Mediterranean. False civil GPS signals from the research team were able to slowly overpower authentic GPS signals to obtain control of the ship's navigation system. According to Professor Todd Humphreys, author of the study, "The ship actually turned and we could all feel it, but the chart display and the crew saw only a straight line" [3], [4]. It is important to note that the GPS and navigation systems impacted were essentially the same as those used throughout commercial maritime operations and the Marine Transportation System, generally. "White Rose of Drax" was not a "soft target." Since so many vessels depend crucially on GPS and other Global Navigation Satellite System (GNSS) signals for navigation as well as surveillance and other functions, this demonstration by Professor Humphreys and his team should raise an alarm. However, a realistic analysis of the threat underscores the need for both proximity and persistent presence required for this attack to work. It can't be done remotely.

*The work of Dr. DiRenzo represents his own views and not those of the US Coast Guard. Dr. Roberts thanks the US Department of Homeland Security (DHS) for its support of the CCICADA Center, a DHS University Center of Excellence at Rutgers University, under Grant 2009-ST-061-CCI002-06.

Modern ships are dependent on a proliferation of sophisticated technology, such as ECDIS (Electronic Chart Display and Information System), AIS (Automatic Identification System), Radar/ARPA (Radio Direction and Ranging) (Automatic Radar Plotting Aid), Compass (Gyro, Fluxgate, GPS and others), Steering (Computerized Automatic Steering System), VDR (Voyage Data Recorder –"Black Box"), GMDSS (Global Maritime Distress and Safety System) and numerous other advanced units and systems. All of these systems are potentially open to cyber attacks.

Consider for example the Electronic Chart Display and Information System (ECDIS), a computer-based navigation system that is an alternative to paper navigation charts. ECDIS integrates a variety of real-time information and serves as an automated decision aid, continuously determining a ship's position in relation to land, charted objects, navigation aids and unseen hazards. ECDIS includes electronic navigational charts and integrates position information from GPS and other navigational sensors, e.g., radar, fathometer and automatic identification systems (AIS). ECDIS may also display additional navigation-related information, such as sailing directions. Use of such a system enables a significant reduction in the crew of today's modern ships, even allowing for "solo watchstanding." To illustrate this point, we note that the world's largest container ship, the Triple-E Maersk, is under construction and will be launched soon. It will have the capacity for 18,000 containers and will be 400 meters long. Yet, it is designed to operate with 13 crew members thanks to ECDIS and other automated systems that could be compromised by cyber-attack [5]. (The Royal Caribbean's Allure of the Seas cruise ship, launched in 2010, is not far behind in size, at 360 meters, and with a capacity of up to 6,360 passengers [6].)

ECDIS flaws could allow an attacker to access and modify files and charts on board or on shore. The result of modified chart data would be unreliable and potentially dangerously misleading navigation information. That could lead to a mishap resulting in environmental and financial damage.

In January 2014, the NCC Group tried to penetrate an ECDIS product from a major manufacturer. Security weaknesses such as ability to read, download, replace or delete any file stored on the machine hosting ECDIS were found. Once such unauthorized access is obtained, an attacker could interact with the shipboard network and everything to which it is connected, causing chaos. Such an attack could be made through something as basic as insertion of a USB key or through download from the internet. (See [7].)

Automatic Identification System (AIS) transceivers are on close to a million ships. Per International Maritime Organization agreement, installation is mandatory for all passenger ships and commercial (non-fishing) ships over 300 metric tons. AIS tracks ships automatically by electronically linking data with other ships, AIS base stations, and satellites. This system enables ships to share positional data with other ships. It offers awareness about those operating within the MTS [8]. An attacker could exploit weaknesses in AIS and falsify a vessel's identity or type, or its position, heading, and speed [9]. As pointed out in [7,10], such an attack could also create a phony vessel (recognized as real) at any location, trigger a false collision warning system alert (resulting in a course adjustment or worse), or create a false weather report leading a ship to change course. It could also impersonate authorities and trick the crew into disabling their AIS, which would make the ship invisible to authorities and others (except attackers). It could flood mariner authorities or other vessels with AIS data, which is essentially what the cyber security literature calls a denial of service attack. In [11], Balduzzi and Pasta give examples of types of attacks on AIS. One is a "frequency hopping attack." In such an attack, an attacker would take advantage of the fact that port authorities can instruct a vessel's AIS to work on a specific frequency. The attacker would spoof the command to operate over a specific frequency, which would be blank. This would cause the vessel to stop sending and receiving on the correct frequency – it would effectively disappear and be unable to communicate. In a "timing attack" (replay attack) the attacker would spoof the command to delay transmission time, and repeat this, again effectively causing the vessel to disappear. (The reverse of this is the denial of service attack mentioned above.) It is reported in [12] that the Somali pirates prompt ships to turn off their navigational devices or fake data so it looks like they are somewhere else. In October 2013, Balduzzi, Wihoit, and Pasta [10] demonstrated how easy it is to penetrate a ship's AIS.

Why is this so easy? The problem arises from the fact that all AIS information is automatically assumed to be genuine. There is no built-in security or verification system that provides a level of backup. Moreover, there is no encryption of AIS messages so they can easily be manipulated [7]. This does suggest potential countermeasures to AIS vulnerability, such as adding authentication in order to ensure that the transmitter is the owner of the vessel, creating a way to check AIS messages for tampering, adding time checking to counter replay attacks, or adding a validity check for data such as geographical information that appears in a message [8].

The example of the spoofing attack on the "White Rose of Drax" showed that this type of activity impacts GPS and could impact the operations of modern ships. As noted in [4], such attacks take advantage of the fact that civil GNSS (in contrast to military GPS) waveforms are unencrypted and unauthenticated. Loran-C, which had been a widespread backup to GNSS, was discontinued in 2010.

In 2008, in another demonstration, The UK & Irish General Lighthouse Authority, in collaboration with the UK Ministry of Defence (MOD) Defence Science and Technology Laboratory (DSTL), directed GPS jamming equipment at a specific patch of ocean. The MN Pole Star sailed into that patch and the jamming succeeded in causing failure in a variety of systems: the AIS transponder, the dynamic positioning system, the ship's gyro calibration system and the digital selective calling system. The ship's ECDIS was not updated due to the GPS failure, and so the screen remained static. In this case, because the crew was expecting the attack, it was able to deal with multiple alarms. One can only imagine how, in a modern ship like the huge Maersk ship described above, where the bridge might be manned by a single person at night, such a jamming attack could lead to major problems. A similar problem might arise if such a jamming attack took place during a highly complex maneuver requiring high concentration, such as docking under very low visibility [7, 13]. Of special concern is that such GPS jamming is possible with low cost jammers available over the Internet (though not legally) at a price as low as $20 apiece.

One goal of the study by the UK & Irish General Lighthouse Authority [13] was to investigate the effectiveness of alternative sources of position, navigation and timing for ships that are complementary to GPS. This is especially important in the light of the decision to not maintain formal support of Loran-C mentioned above. In particular, [13] describes the complementary nature of Enhanced Loran (eLoran), which has failure modes dissimilar to those of GPS. It describes satisfactory performance of an eLoran receiver in the area where GPS service was jammed and justifies the effort to introduce eLoran in the UK.

III. OIL RIGS

The vulnerabilities described above are not limited to ships. They extend to the entire MTS. For example, according to security company ThetaRay, a cyber attack on a floating oil rig off the coast of Africa managed to tilt the rig slightly and as a result it was forced to shut down. It took a week to identify and fix the problem [7, 12].

In 2010 a drilling rig being moved at sea from South Korea to South America was infected by malicious software. The result was that its critical control systems could not operate and it took 19 days to fix matters [7,12]. Among other things, the cyber attack infected the computers controlling the blowout preventer. If this had happened in conjunction with a loss of dynamic positioning and an emergency breakaway, the results could have been disastrous (the blowout preventer failed during the Deepwater Horizon oil spill in the Gulf of Mexico in 2010.) The malware of the type involved might not have caused a problem for a smart phone, but could have caused a devastating impact for an oil rig which does not have up to date security measures [14].

The system that keeps an oil rig in position may also have vulnerabilities. Dynamic positioning (DP) is a computer-controlled system to automatically maintain the position (and heading) of a vessel, and in particular of an oil rig. DP is used by much of the offshore oil industry. In DP, knowledge of the oil rig's position and angle, sensor information, wind direction and speed, and other factors feed into a computer program that, among other things, contributes to the stability of the rig. An enhanced Differential GPS is used [15]. Disabling the DP of an oil rig, for example by jamming its GPS, especially if it were coupled with a relatively simple hydrophone that could also disrupt the rig's sonic transponders on the seafloor, would conceivably have a very serious effect on the rig.

In addition to the potential safety and environmental impacts of an oil rig failure, there is a potentially large cost involved. Oil rigs are contracted for at prices approaching ¾ of a million dollars a day [14].

IV. CARGO

Modern port operations, around the world, are heavily dependent on complex networked logistics management systems that track maritime cargo from overseas until it has reached a retailer. Yet, these systems are subject to cyber attacks that can cause significant problems. For example, the Port of Antwerp, Belgium, is one of Europe's largest and, indeed, one of the biggest in the world. Like most modern cargo handling systems, its system allocates a reference number to each container so it can be tracked upon entry to the port, it can be located while in the port waiting to be picked up, and the operators can know when it is due to be picked up [16]. In the period 2011 to 2013, hackers infiltrated computers at the Port of Antwerp. This enabled them to locate specific containers, find the security code for a container, change the location and scheduled delivery time, and make off with smuggled drugs before the scheduled pickup. In this way, through remote access to terminal systems, the criminals could release containers to their own truckers without either the port or the shipping line knowing. Indeed, they could delete information about the very existence of a container [7,12,16,17]. Apparently, the hackers began by emailing malware to the port authorities and/or shipping companies (a "spear phishing" attack). After the infection was discovered and a firewall installed to prevent further infections, the criminals broke into the facility housing the cargo-handling computers and fitted devices that enabled them to gain wireless access to keystrokes and get screen shots of computer screens, which enabled them to continue their operations [16,18,19].

In 2012, it was revealed that a different kind of cyber crime was committed in Australia. In this case, criminals were able to hack into the cargo systems that were operated by Australian Customs and Border Protection. This allowed the criminals to determine whether or not a shipping container was regarded as suspicious by the authorities. They could then simply abandon those containers considered suspicious and concentrate on containers that were not on the radar screen of the police [7].

A third example involves the Iranian shipping line IRISL A cyber attack in 2011 damaged data related to loading, cargo number, data and place. Indeed, the shipping line then did not know the location of containers, e.g., whether they were onboard or onshore, or whether they had at one time been loaded onto a ship. This led to cargo losses, sending cargo to the wrong destinations and other major disruptions in operations [7].

The United States Federal Bureau of Investigation has advised private industry that GPS jammers are a common tool for cargo theft by organized crime. In their July 2014 advisory [20] they report 46 instances of jammer use transporting stolen cars to China, and one instance of the theft of a trailer of refrigerated pharmaceuticals.

V. PORT OPERATIONS

Cargo handling is at the heart of port operations, but the system tracking cargo is not the only port system that is subject to cyber attack. Today, ports rely as much on computer networks as on stevedores lifting and hauling goods. Special network control systems control the loading and unloading of cargo. All kinds of devices such as gantry cranes now use technologies such as optical recognition to manage port operations, including locating cargo, transporting it, inspecting it, etc. Containers are automatically placed and moved using GPS [21]. Trucks that haul cargo away from the port are also heavily dependent on GPS. This modern port operating system makes the entire port vulnerable. Indeed, easily available GPS jammers could potentially close down the entire port, from cargo handling to truck and crane movement. The cost of shutting down a port for just one day has been estimated to be on the order of somewhere between $1B and $2B a day (counting effect on the GDP regionally and nationally) [2,22], though the exact cost is challenging to quantify. At least one instance of GPS disruption having a major impact on port operations has been reported. Sometime in 2014, two cranes at a major US east coast port were idled for 7 hours when they were unable to receive GPS signals. [23]

VI. CONCLUDING COMMENTS

The cyber threats to the maritime domain we have described are serious and they are not well known. In November 2011, the European Network and Information Security Agency (ENISA) reported that, "[t]he awareness on cybersecurity needs in the maritime sector is currently low to non-existent" [24]. In its report, ENISA recommended maritime sector awareness raising and cyber security training of shipping companies, port authorities, and national cyber security offices. It also recommended updating regulations and policies from an exclusive emphasis on physical aspects of security in the maritime domain to cyber aspects.

A 2013 Brookings Institution Report [21] found that of the six ports studied, only one had conducted a cyber security vulnerability assessment and not a single one had a cyber incident response plan.

A 2014 report by the US Government Accounting Office (GAO) [25] found that the US Department of Homeland Security needs to better address maritime cyber security (in particular port cyber security) and asked that the US Coast Guard assess cyber-related risks and use the assessment to inform maritime security guidance.

Is the maritime transportation system "special" in its cyber threats? In some ways it is, for example given the long distances from land, dependence on long-range communications systems, and dependence on specialized instruments for position, navigation, and timing. However, mostly the issues we have raised involve lack of awareness by management, lack of information about attacks and vulnerabilities, emphasis on physical security, lack of cyber security training of personnel - issues that are similar to those facing many other areas. What is clear is that the maritime transportation industry can and should learn from other industries and that there is need to spread awareness of the maritime cyber threat.

We have concentrated in this paper on a statement of the problem, not on the potential solutions to it. Responsibility for identifying and implementing solutions seems to be a shared responsibility between the commercial entities and the government. Vessel and facility owners must ensure their personnel are properly trained and equipped to deflect and quickly recover from cyber attack as part of an over-arching risk management effort that looks to threats, vulnerabilities and consequences. For its part, the government must coordinate best practices, quickly share information when it becomes available, and ensure that fundamental maritime utilities, like GPS and AIS, are properly protected, toughened and augmented. It is also clear that more research is needed on the development of modern cyber-physical systems (CPS), engineered systems that are built from and depend upon the synergy of computational and physical components.

ACKNOWLEDGMENTS

The authors thank CAPT David Moskoff, US Merchant Marine Academy, for the many ideas that led to this paper.

They also thank CAPT Michael Dickey, US Coast Guard, and CAPT Andrew Tucci, US Coast Guard, for detailed comments on earlier drafts.

REFERENCES

[1] United States Coast Guard, Western Hemisphere Strategy, September 2014.

[2] "West Coast Port Congestion Could Cost Retailers $36.9 Billion in the Next 24 Months," Business Wire, Feb. 7, 2015, http://www.businesswire.com/news/home/20150207005007/en/West-Coast-Port-Congestion-Cost-Retailers-36.9#.VPiNIsbA7c8, accessed March 5, 2015.

[3] S. Zaragoza, "Spoofing a Superyacht at Sea," Know, University of Texas at Austin, May 5, 2014.

[4] J. Bhatti and T.E. Humphreys, "Covert control of surface vessels via counterfeit surface GPS signals," unpublished.

[5] "Triple-E: The world's largest ship," http://www.worldslargestship.com/, Maersk, accessed Jan. 1, 2015.

[6] "The biggest cruise ships in the world," Cruise Critic, http://www.cruisecritic.com/articles.cfm?ID=1431, accessed March 5, 2015.

[7] CyberKeel, Maritime Cyber-Risks, Oct. 15, 2014, http://www.sfmx.org/support/amsc/cybersecurity/webdocs/Maritime%20Cyber%20Crime%2010-2014.pdf, accessed Jan. 1, 2015.

[8] "Digital ship pirates: Researchers crack vessel tracking system," Net Help Security, October 16, 2013, http://www.net-security.org/secworld.php?id=15781, accessed Feb. 21, 2015.

[9] S. Mullin, "Cyber resilience in the maritime and energy sectors," Templar Executives, May 1, 2014, http://www.templarexecs.com/cyberresilience/, accessed Feb. 21, 2015.

[10] M. Balduzzi, K. Wihoit, A. Pasta, "Hey Captain, where's your ship? Attacking vessel tracking systems for fun and profit," 11th Annual HITB Security Conference in Asia, http://conference.hitb.org/hitbsecconf2013kul/materials/D1T1%20-%20Marco%20Balduzzi,%20Kyle%20Wilhoit%20Alessandro%20Pasta%20-%20Attacking%20Vessel%20Tracking%20Systems%20for%20Fun%20and%20Profit.pdf, accessed Feb. 21, 2015.

[11] M. Balduzzi, A. Pasta, K. Wihoit, "A Security Evaluation of AIS Automated Identification System," http://www.iseclab.org/people/ embyte/papers/ais_acsac14.pdf, accessed Feb. 21, 2015.

[12] J. Wagstaff, "All at sea: Global shipping fleet exposed to hacking threat," April 23, 2014, Reuters, http://www.reuters.com/article/2014/04/23/tech-cybersecurity-shipping-idUSL3N0N402020140423, accessed Feb. 21, 2015.

[13] A. Grant, P. Williams, N. Ward, and S. Basker. GPS jamming and the impact on maritime navigation. *Journal of Navigation*, *62*(02), 173-187. 2009.

[14] Z. Shauk, "Malware offshore: Danger lurks where the chips fail," April 29, 2013, http://fuelfix.com/blog/2013/04/29/malware-offshore-danger-lurks-where-the-chips-fail/, accessed Feb. 21, 2015.

[15] "Dynamic positioning, "http://en.wikipedia.org/wiki/Dynamic_positioning, accessed Feb. 21, 2015.

[16] S. Bell, "Cyber-attacks and underground activities in Port of Antwerp," Bull Guard, Oct. 21, 2013, http://www.bullguard.com/ blog/2013/10/cyber-attacks-and-underground-activities-in-port-of-antwerp.html, accessed Feb. 21, 2015.

[17] "To move drugs, traffickers are hacking shipping containers," Motherboard, Oct. 21, 2013, http://motherboard.vice.com/blog/how-traffickers-hack-shipping-containers-to-move-drugs, accessed Feb. 21, 2015.

[18] J. Mulrenan, "How hackers attacked the Port of Antwerp," TradeWinds, Aug. 1, 2014, http://www.tradewindsnews.com /weekly/342065/How-hackers-attacked-the-Port-of-Antwerp, accessed Feb. 21, 2015.

[19] "Cyber-attacks; a new tool for drug traffickers," Woodland Group, http://www.woodland-group.com/news/display/cyber-attacks-a-new-tool-for-drug-traffickers/402/60, accessed Feb. 21, 2015.

[20] Federal Bureau of Investigation, "FBI Cyber Division Bulletin: Cargo thieves use GPS jammers to mask GPS trackers," https://publicintelligence.net/fbi-cargo-thieves-gps-jammers/, accessed March 5, 2015.

[21] J. Kramek, "The critical infrastructure gap: U.S. port facilities and cyber vulnerabilities," Federal Executive Series Policy Papers, Brookings Institution, July 3, 2013.

[22] M. Orsosz, et al., "Protecting our nation's ports with the port security risk analysis and resource allocation system (PortSec 3.0)," Proceedings IEEE Conference on Technologies for Homeland Security (HST), 2010, pp. 264-269.

[23] "GPS disruption halts ports, endangers ships – US Coast Guard," Resilient Navigation and Timing Foundation, Feb. 11, 2015, http://rntfnd.org/2015/02/11/gps-disruption-halts-ports-endangers-ships -us-coast-guard/, accessed March 5, 2015.

[24] European Network and Information Security Agency, Analysis of Cyber Security Aspects in the Maritime Sector, November 2011.

[25] US Government Accounting Office, Maritime Critical Infrastructure Protection: DHS Needs to Better Address Cybersecurity, GAO 14-459, June 5, 2014.