Spring 2019

Cybersecurity in the Maritime Domain

Gary C. Kessler
Embry-Riddle Aeronautical University, kessleg1@erau.edu

The Coast Guard Journal of Safety & Security at Sea

PROCEEDINGS

Spring 2019 of the Marine Safety & Security Council

PROCEEDINGS

Spring 2019 Vol. 76, Number 1

75th Anniversary of *Proceedings*

6 **The MSSC and Proceedings** | A story 75 years in the making
by Samantha L. Quigley

12 **Ready, Relevant, and Evolving** | The 75-year evolution of the Coast Guard's marine safety mission
by LCDR Luke Petersen and Maggie Chan, Ph.D.

17 **A Short History of IMO's Maritime Safety Committee**
by International Maritime Organization

21 **The Role of Marine Science and Oceanography in the United States Coast Guard**
by Jonathan Berkson, Ph.D., CDR William Woityra, CDR Kenneth Boda, Arthur Allen, Michael Hicks, and LCDR Victoria Futch

30 **Icebreaking History, Platforms, and Activities**
by CDR William Woityra

34 **Cybersecurity in the Maritime Domain**
by Gary C. Kessler

80th Anniversary of the Coast Guard Auxiliary

46 **USCG Auxiliary's Proud Heritage and Continuing Mission** | 80 years of service to the Coast Guard and the boating public
by C. Douglas Kroll, Ph.D.

52 **The History of Coast Guard Auxiliary Aviation** | More than 70 years of service
by Joseph Giannattasio

Dawn over the Atlantic Ocean's Coast Guard Beach on Cape Cod National Seashore, Massachusetts. Under Vice Admiral R.R. Waesche, the Coast Guard station located here was rebuilt and formally manned beginning January 9, 1937, until its decommissioning and departure of crew September 15, 1958. Today, it is used as an educational and residential facility for NEED—the National Environmental Education Development Program. Photo by Danita Delmont | Shutterstock.com

56 **Hunting for *Bear*** | The search for the Coast Guard's most iconic vessel
by Mark A. Snell, Ph.D.

61 **The Coast Guard Auxiliary Interpreter Corps** | A valuable asset
by Keith Fawcett

On Deck

4 **Assistant Commandant's Perspective**
by Rear Admiral Steven J. Andersen

4 **Commodore's Perspective**
by Commodore Larry L. King

40 Historical Snapshot
The Long Blue Line | *Jackson*'s battle with the rogue waves of '44
by William H. Thiesen, Ph.D.

64 Chemical of the Quarter
Understanding Ammunition
by Ms. Hillary Sadoff

Nautical Queries
65 **Engineering**
67 **Deck**

On the Cover: *What began as the Merchant Marine council in January 1944, has endured 75 years of change. The coin on the cover represents the evolution of regulations, policies, and scope of operation, as well as the resiliency of what today is known as the Marine Safety and Security Council and* Proceedings. *Weathering the change for 62 of those 75 years is the icebreaker U.S. Coast Guard Cutter* Mackinaw *(WAGB-83) on the back cover. Built during World War II, it allowed for expedited winter shipping of steel. Decommissioned in 2006, "The Queen of the Great Lakes," is now a maritime museum in Mackinaw City, Michigan.*

Butus | Shutterstock.com

Proceedings is published three times a year in the interest of safety at sea under the auspices of the Marine Safety & Security Council. Special permission for republication, either in whole or in part, except for copyrighted material, is not required, provided credit is given to *Proceedings*.

Editorial Contact

Email: HQS-DG-NMCProceedings@uscg.mil

Mail Commandant (CG-5PS)
ATTN: Editor, *Proceedings* Magazine
U.S. Coast Guard Stop 7318
2703 Martin Luther King Jr. Ave. S.E.
Washington, DC 20593-7318

Web: www.dco.uscg.mil/proceedings

Phone: (202) 372-2316

Subscription Requests

Proceedings is free of charge and published in April, August, and December.

Subscriptions:
www.dco.uscg.mil/proceedings

Cybersecurity in the Maritime Domain

by Gary C. Kessler, Ph.D.
Professor of Cybersecurity
Embry-Riddle Aeronautical University

Editor's Note: The majority of the articles in this issue address safety and prevention programs and policies that have developed since the inception of the Coast Guard and are at the core of its mission. Today, that mission has evolved to include safety and prevention in cyberspace. It is feasible that when Proceedings marks its 100th anniversary, cybersecurity be as much a core safety and prevention mission as ice breaking. This article describes the cybersecurity challenges and strategies currently facing the maritime industry.

In 2017 and 2018, the maritime industry saw a record number of attempted—and many successful—frauds via email, phishing, or other means. Demonstrated and actual attacks on vessel networks, communication systems, and navigation systems have become practically routine. Port and shipping line networks are increasingly vulnerable to what appears to be increasingly targeted attacks against maritime systems.

The global marine transportation system (MTS) is huge, complex, and uses myriad technologies with a wide range of sophistication. Maritime systems are commonly designed to accommodate predictable failures—e.g., material fatigue due to age and use—but not intelligent actors. There is, and can be, no central management of maritime cyber systems, hence every player has to manage their own network and protect themselves from everyone else. Of course, the maritime industry has some of its own unique cyber vulnerabilities.

An Overview of the Maritime Cyber Landscape

The United States' marine transportation system includes 25,000 miles of navigable channels and waterways, more than 4,100 ports and marinas, 200 ferry operations, and 238 locks. It also includes 12 million recreational boats and tens of thousands of commercial, merchant, military, municipal, and other vessels. Shipping, the method by which 90 percent of global trade moves, is also this country's primary mode of transportation for the import and export of goods.

Information security threats to the maritime industry are not much different than threats to the general world of computer and network technology. Viruses, worms, and other forms of malicious software, or malware, affect the industry even when shipping is not the direct target. Stuxnet, for example, the circa-2009 malware targeting centrifuges used in Iranian nuclear research facilities, was also found in control systems at Chevron.[1] NotPetya, the ransomware virus that spread across the planet in a matter of hours in May 2017, cost Maersk Line as much as $300 million in lost revenue, forcing them to rebuild nearly 50,000 servers and user computers—and Maersk wasn't even a target, merely vulnerable.[2]

This is not to say that the maritime industry has not been targeted. Advanced persistent threats (APT)—a class of attack first described in 2010—are cyberattacks targeting a specific victim using sophisticated, dynamic methods that adapt to the victim's defenses, and are often state-sponsored. Reports in 2018 showed that Chinese-linked APTs had been targeting the maritime industry since 2013, with particular escalation in 2017.[3]

Cyberattacks on maritime information technology (IT) systems have been ongoing for some time. Hackers broke into Australian Customs and Border Protection Service cargo management systems in 2012 to track illicit cargo, allowing them to alert criminals if their particular containers had been marked as suspicious by the customs service. From 2011–2013, hackers used a variety of methods to break into Port of Antwerp the computer systems controlling movement and location of shipping containers, allowing criminals to generate bogus bills of lading, allowing them to remove cargo containers before the legitimate owner arrived.[4] In 2016, hackers exploited one shipping company's content management system, allowing pirates to identify specific containers on specific vessels, enabling them to target desired cargo ships and get on and off the vessel in a matter of hours.[5]

Cyberfraud is also a serious concern in the industry due to the high volume of communications, orders, and financial transactions that occur online. In 2014, World Fuel Services was defrauded of $17.9 million by a bogus fuel order, and a Malaysian bunker company was defrauded of more than $1 million in a phishing scheme.[6] In 2015, a shipping company in Cyprus received a fuel bill for $644,000 with a request to send the payment to a

different bank account than usual. A criminal had sent a bogus bill for a legitimate order and misdirected the funds to their account.[7]

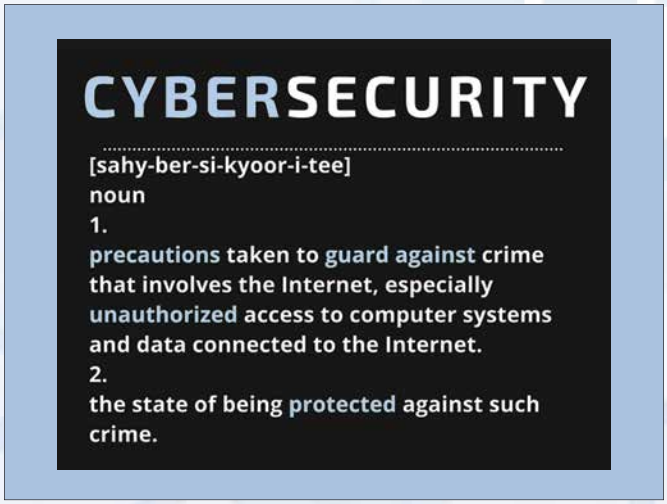
Presumably, every IT system manager in the industry has taken steps to protect their computers, servers, mobile devices, control systems, and other digital equipment from the threats associated with poor cybersecurity. Even so, cybersecurity policies and procedures specific to the maritime industry are still in the early stages, and there is only a very limited systematic response.

The Maritime IT System of Systems

There are myriad IT systems, components, vendors, jurisdictions, and manufacturers, as well as organizational policies, procedures, and requirements within the MTS. It is this diversity that makes protecting maritime IT assets from cyberthreats so difficult. Consider that the maritime system and industry comprises the following components and vulnerabilities:

- *Seaport operations,* including vessel control and traffic management, personnel management and screening, passenger management and passport control, WiFi and physical networks
- *Cargo and shipping,* including logistics, supply chain, routing, scheduling, loss management
- *Manufacturing,* including intellectual property theft, supply chain, payment systems, software and hardware flaws
- *Vessel traffic management,* including ship management, routing, communication, location management and communication
- *Shipping line operations,* including passenger information, reservation systems, communication, baggage and cargo handling, maintenance, catering, payment systems
- *Vessel operations,* including the ship's onboard network architecture providing interconnection between the bridge navigation, communication, mechanical, ship monitoring and security, cargo handling and other specialized systems, and communication with external networks with regards to vessel traffic management, ports, and shipping lines
- *Unmanned/autonomous vehicles,* including remote control or monitoring, GPS hacking and jamming, hardware and software flaws

At one level, these individual systems can be thought of as regular computers and networks. They are therefore susceptible to the same threats as any other computer or network, especially when it comes to human "weak links" in the system who will make errors or don't follow processes and procedures. Indeed, human error—clicking on a fateful web link, opening a malware attachment in an email, plugging a USB thumb drive of unknown origin into a computer, or not keeping up-to-date with anti-malware software—causes most cyber incidents. Even worse, intentional human attackers, including cybercriminals, cyberspies, and state-sponsored cyberterrorists, prey upon this lack of vigilance to force and/or exploit those human and system errors.



Air Force Special Operations Command

One result of the interconnectedness of networks within a system is that one network provides a path to other networks. For example, in late 2017 maritime cyber consulting company Naval Dome reported on multiple vulnerabilities in a shipboard network.[8] In one case, malware was inserted into the vessel's Electronic Chart Display and Information System (ECDIS) via a satellite link to the master's computer. Unbeknownst to the crew, the malware altered the ship's position during the night without changing the ECDIS display. A second piece of malware was uploaded to the radar system via the network switch that connected radar, ECDIS, bridge, and other ship communication systems. This malware altered the radar display by deleting targets on the display, essentially blinding the ship. The final malware was inserted into the machinery control systems network via an infected thumb drive.

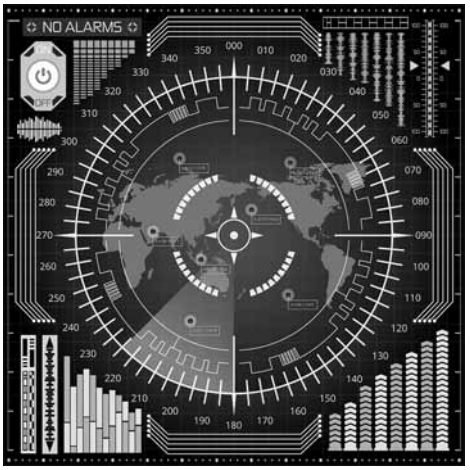
At another level, the issue lies not in protecting an individual system or network, but in the difficulty of protecting the broader system of systems and the inherent complexities therein. The networks throughout the MTS are ultimately interconnected, so the ripple effect of an attack on one part of the system might be felt in other parts. Even if every component within a single system or network was proven to be totally immune to attack, it would be impossible to ensure the security of all of those interconnected components. This is further complicated by the fact that no organization has any control over the other networks with which they interact. A common strategy of groups engaged in an APT is to probe and perform reconnaissance to find the weakest link in a set

of interconnected networks, or to attack a target's supply chain partners, in order to identify a pathway to the ultimate target.[9]

Cyber Threats to Navigation Systems

The global positioning system (GPS) and other global navigation satellite systems (GNSS) are essential elements to safety within the MTS. In addition to its obvious uses in navigation and ship positioning, GPS provides data for the placement of aids to navigation, chart surveys, ECDIS displays, and radar. GPS signals are transmitted from medium Earth orbit satellites at an altitude of 12,000–15,000 miles. Overpowering these relatively weak, unencrypted signals is not hard. In 2013, a University of Texas at Austin team demonstrated the ability to spoof GPS signals to cause a ship's crew to deviate course in a proof-of-concept experiment using off-the-shelf equipment.[10]

Deliberate GPS spoofing attacks have caused ships' equipment to misreport—or lose—their own position or that of other ships. In June 2017, a mass GPS spoofing incident in the Black Sea targeted ships off the Russian port of Novorossiysk, causing their GPS-based navigation systems to report their location up to 25 miles away at the Gelendzhik Airport. A secondary side effect involved the ships' automatic identification systems (AIS) broadcast alerts as they found themselves within 100 meters of at least a dozen other ships—all believing that they were at the same airport. This incident was thought to be the result of a Russian electronic warfare exercise.[11] These types of activities continue, with multiple GPS spoofing incidents reported in the eastern Mediterranean Sea during the first half of 2018.[12]



Eugenius777 | Shutterstock.com

The AIS is a GPS-based vessel tracking system providing a ship's unique identifier, position, course, speed, and other information. In a busy harbor or traffic lane, it broadcasts a ship's position and displays the location of other ships in the area. Cybersecurity solutions company TrendMicro has reported on several vulnerabilities in AIS, including the lack of message validity, integrity, authentication, and timing checks, and lack of encryption.[13] AIS also responds to abnormal events. For example, an attacker could cause a ship's crew to change course by spoofing the AIS' closest point of approach (CPA) warning, another ship's AIS distress beacon, or dynamic weather information. There are many reasons an attacker might want to divert a ship—from wanting to run it aground, to bringing it closer to pirates, to charging a ransom to *not* do these things.

Several public websites and smartphone apps allow anyone to find the current location of any vessel broadcasting its AIS information. The International Maritime Organization (IMO) Maritime Safety Committee warned against the dangers of AIS-based information leakage as far back as 2004. Even then, the IMO recognized that posting AIS on web pages and other public sites had the potential to undermine the safety of navigation and security in the international MTS.[14]

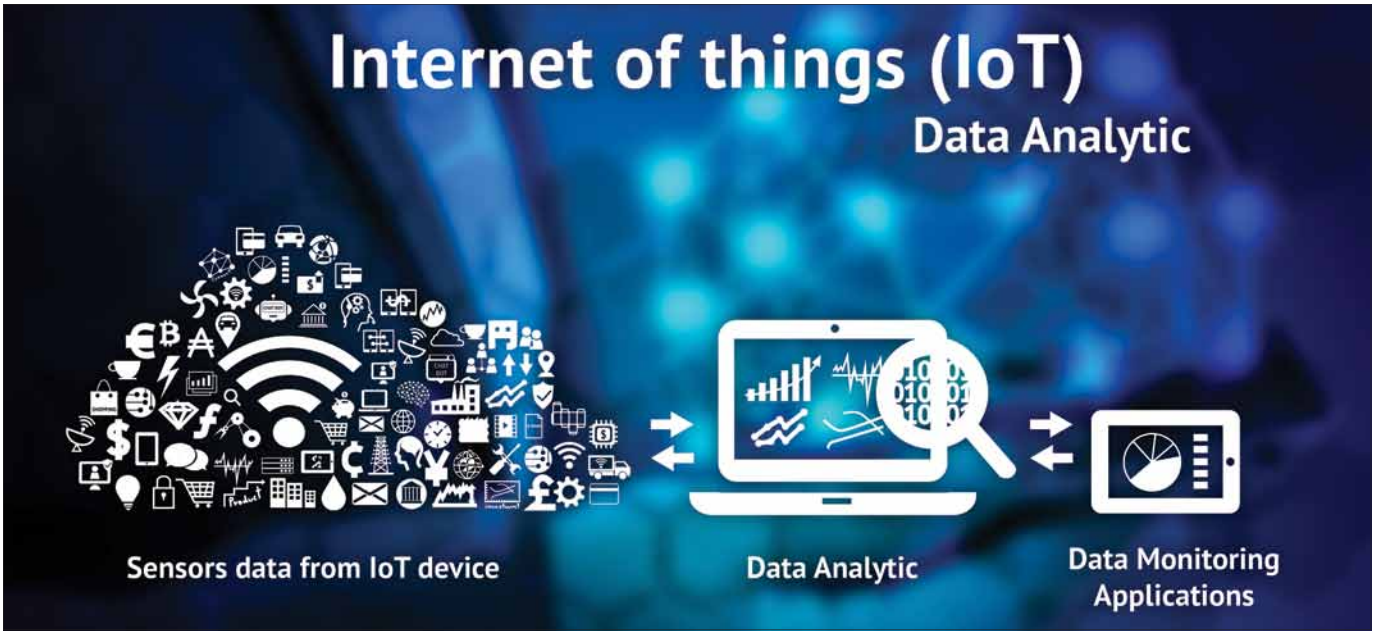
> Timing is critical to global positioning given that a one-nanosecond—one billionth of a second—error is equivalent to approximately one foot of positioning error.

Cyber Threats to Autonomous and Smart Systems

The introduction and growing use of automation in ships, ports, cargo, operations, and other maritime systems has added tremendous efficiencies and cost savings. It has also removed the possibility of human interference from many aspects of the redundancy and control loop.

A growing trend in the MTS is the development of so-called *smart ports*, largely using internet of things (IoT) technology. Smart ports use network-attached sensors to monitor tide, current, temperature, wind direction/speed, water depths, visibility, berth availability, and other data, feeding a centralized information dashboard to connected vessels. This type of system can streamline port operations to reduce wait times; optimize dock, load, and unload times; and maximize the number of vessels that can be managed efficiently, allowing the port and shippers to save significant amounts of money. Security, however, is not built into the design and development of these low-cost IoT devices, making them notoriously subject to network-based attacks. The massive distributed denial-of-service in 2016 against domain name and email service provider Dyn, for example, was due to a botnet—an automated attack network—comprising more than 100,000 such devices.[15]

Autonomous and remote-controlled vessels and port vehicles are another growing trend in the maritime industry, as witnessed by the Maritime Unmanned



Zapp2Photo | Shutterstock.com

Navigation through Intelligence in Networks initiative and projects being led by organizations like Massterly, Rolls-Royce, the Port of Long Beach, and the Maritime Port Authority of Singapore. The technology that would support this level of automation is definitely in place, but what is missing is enough trust that these systems cannot be compromised via network attacks.[16]

Cyberphysical Threats

Cyberattacks are generally thought of as events that use a cybervector towards a cybertarget. Cyberphysical threats specifically address the case where the cyber vector is targeting a physical asset. Indeed, cyberphysical systems, defined as those that integrate computers and physical components, are increasingly common in all aspects of our lives as we develop more sophisticated sensors, instruments, networks, and embedded computers.[17] In the MTS environment, consider the situation if cyberterrorists were to gain control of autonomous vehicles at a port and use them to "attack" people or damage equipment at the port.

More worrisome is the case of gaining access to a ship's navigation, propulsion, or ballast system. If a ship could be deliberately grounded in any number of critical locations, the increase in shipping costs caused by delays or rerouting would be enormous, not to mention the cost to repair damaged facilities. If an attacker could alter sensors, gauges, or containment systems on a vessel carrying potentially hazardous materials, it might be possible to create a spill, explosion, or other adverse action.

Ultimately, all cyberattacks have a physical target, whether directly or indirectly. What has not been addressed yet is this scenario: If we would not allow a vessel of people with infections to a public dock, why would we not quarantine a vessel with a network virus, prevent them from connecting to a port's network? We need to take seriously cyberthreats to vessels, ports, and other parts of the MTS, and isolate "sick" entities from the "healthy" ones.[18]

Conclusion

The maritime industry is constantly evolving to become more advanced, compared to its ancient roots. Unfortunately, many old technologies, processes, and procedures in place today haven't kept up, causing some executives in the industry to observe that the maritime industry is 30 to 500 years behind in terms of technology.[19] This makes it difficult to keep up with the rapid acceleration of change—not only the adoption of new technology, but of understanding the vulnerabilities, exploits, and risks of emerging technologies.

A number of maritime industry organizations are responding to cyberthreats via suggested policies and procedures. The Baltic and International Maritime Council guidelines for vessel cybersecurity, for example, take a risk management approach to vessel cybersecurity.[20] The American Bureau of Shipping guidelines apply best practice cybersecurity principles to ships and other maritime platforms, as well as the landside systems that support them.[21] The National Institute of Standards and Technology, in conjunction with the U.S. Coast Guard, has added maritime-specific profiles to its widely used cybersecurity framework documents.[22] Indeed, the USCG Academy started a cyber systems major in fall 2018, their first new major in 20 years.[23] In addition, a private company specializing in testing,


AliceAbob | Shutterstock.com

inspection, and certification, has released cybersecurity guidelines addressing software management and secure ship-to-shore communication.[24]

Despite all of these measures, a 2017 industry survey about maritime cybersecurity revealed a disparity between management and crewmembers. While two-thirds of executives and managers think their organization provides cybersecurity awareness for crew and staff, less than half of the crew and staff respondents still think they receive adequate training. And, while only a third of executives identified insiders as the biggest cybersecurity threat, half the managers and two-thirds of the crew and staff disagreed.[25]

None of the observations made here are a surprise to most cybersecurity professionals. The marriage of the maritime industry and technology is as important as it is inevitable. Facilitation of open discussions will help the industry better prepare for and address information risks inherent with cybersecurity attacks.

About the author:
Gary C. Kessler, Ph.D., is a professor of cybersecurity at Embry-Riddle Aeronautical University in Daytona Beach, Florida, and a cybersecurity consultant with a particular interest in maritime issues. He holds a bachelor of arts degree in mathematics, a master's degree in computer science, and a Ph.D. in computing technology in education. He is also a 50 GT Master and a member of USCG Auxiliary Flotilla 44, District 7.

Endnotes:

1. Chevron Says Hit by Stuxnet Virus in 2010. (2012, November 9). *Phys.org.* Retrieved from https://phys.org/news/2012-11-chevron-stuxnet-virus.html
2. Olenick, D. (2018, January 26). NotPetya Attack Totally Destroyed Maersk's Computer Network: Chairman. *SC Media.* Retrieved from www.scmagazine.com/notpetya-attack-totally-destroyed-maersks-computer-network-chairman/article/739730/
3. Paganini, P. (2018, March 17). Chinese APT Group TEMP.Periscope Targets US Engineering and Maritime Industries. *Security Affairs.* Retrieved from http://securityaffairs.co/wordpress/70355 /hacking/temp-periscope-espionage.html
4. Maritime Industry is Easy Meat for Cyber Criminals. (2015, May 22). *Kaspersky Lab Daily.* Retrieved from www.kaspersky.com/blog/maritime-cyber-security/8796/
5. Sophos. (2016, March 7). Pirates Hacked Shipping Company to Steal Info for Efficient Hijackings. *naked security.* Retrieved from https://nakedsecurity.sophos.com/2016/03/07 /pirates-hacked-shipping-company-to-steal-info-for-efficient-hijackings/
6. Court Backs World Fuel Services Following $17 Million Bunker Theft. (2016, June 9). *Ship & Bunker.* Retrieved from https://shipandbunker.com/news/world/340232-court-backs-world-fuel-services-following-17-million-bunker-theft
7. Birkett, H. (2015, August 27). Hackers Steal $644,000 From a Cyprus Shipping Company. *Splash247.com.* Retrieved from https://splash247.com/hackers-steal-644000-from-a-cyprus-shipping-company/

8. Wee, V. (2017, December 22). Naval Dome exposes vessel vulnerabilities to cyberattack. *Seatrade Maritime News*. Retrieved from www.seatrade-maritime.com/news/europe /naval-dome-exposes-vessel-operational-vulnerabilities-to-cyber-attack.html

9. Reeds, C. (2018, May 13). The Seven Phases of a Cyber Attack. *The Maritime Executive*. Retrieved from https://maritime-executive.com/blog/the-seven-phases-of-a-cyber-attack

10. Spoofing a Superyacht at Sea. (2013, July 30). *UTNews*. Retrieved from https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea

11. Goward, D. (2017, July 11). Mass GPS Spoofing Attack in Black Sea? *Maritime Executive*. Retrieved from https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea

12. Midgett, A. (2018, May 7). U.S. Maritime Advisory 2018-007—GPS Interference in Eastern Mediterranean Sea. *Coast Guard Maritime Commons*. Retrieved from http://mariners.coastguard.dodlive.mil/2018/05/07/5-7-2018-u-s-maritime-advisory-2018-007-gps-interference-in-eastern-mediterranean-sea/

13. Balduzzi, M., Wilhoit, K., & Pasta, A. (2014, December). *A Security Evaluation of AIS*. Trend Micro Research Paper. Retrieved from www.trendmicro.com/cloud-content/us/pdfs /security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf

14. AIS Transponders. (2004, December). Maritime Security—AIS Ship Data. *International Maritime Organization*. Retrieved from www.imo.org/en/OurWork/Safety/Navigation /Pages/AIS.aspx

15. Kan, M. (2016, October 26). DDoS Attack on Dyn Came From 100,000 Infected Devices. *COMPUTERWORLD*. Retrieved from www.computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html

16. Kuhn, K. (2017, May-December). Cyber Risk Management in the Maritime Transportation System. *Proceedings of the Marine Safety & Security Council*, 75(1), 65–69.

17. Serpanos, D. (2018, March). The Cyber-Physical Systems Revolution. *Computer*, 51(3), 70–73.

18. Cook, K.S., & Nichols, D.L. (2017). Cyber Seaworthiness: A Call to Action. In J. DiRenzo III, N.K. Drumhiller, & F.S. Roberts (Eds.), *Issues in Maritime Cyber Security* (pp. 81–85). Washington, D.C.: Westphalia Press.

19. Chambers, S. (2018, March 16). Maritime CEO Forum: Shipping Anywhere From 30 to 500 Years Behind the Technology Curve. *Splash247.com*. Retrieved from https://splash247.com /maritime-ceo-forum-shipping-anywhere-30-500-years-behind-technology-curve/

20. BIMCO et al. (2017, July). *The Guidelines on Cyber Security Onboard Ships*. Retrieved from www.bimco.org/products/publications/free/cyber-security

21. ABS. (2016, September). The Application of Cybersecurity Principles to Marine and Offshore Operations, Vol. 1. Retrieved from ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/250_cybersafetyV1/CyberSafety_V1_Cybersecurity_GN_e.pdf

22. U.S. Coast Guard. Port & Facility Compliance Home, Domestic Ports, Cybersecurity Web page. Retrieved from www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/

23. USCG Academy. (2018, July 10). Cyber Systems major now offered at Coast Guard Academy. USCGA Press Release. Retrieved from https://content.govdelivery.com/accounts/USDHSCG /bulletins/1fd9e8d

24. Bureau Veritas. (2018, March 13). Cyber Safety, Security and Autonomous Shipping Addressed With New Bureau Veritas Notations and Guidelines. Retrieved from www.bureauveritas.com/home/news/business-news/cyber-safety-security-and-autonomous-shipping-addressed-with-new-bureau-veritas-notations-and-guidelines

25. Fairplay. (2017, October 4). Maritime Cyber Security Survey 2017. Retrieved from https://fairplay.ihs.com/safety-regulation/article/4292441/maritime-cyber-security-survey-2017