5-2021

Cross Domain IW Threats to SOF Maritime Missions: Implications for U.S. SOF

Gary C. Kessler
Embry Riddle Aeronautical University - Daytona Beach, gary.kessler@erau.edu

Diane M. Zorri
Embry-Riddle Aeronautical University, Diane.Maye@erau.edu

Iran's Revolutionary Guard inspect the British-flagged oil tanker *Stena Impero*, which was seized in the Strait of Hormuz by the Guard, in the Iranian port of Bandar Abbas. Tensions in the Persian Gulf escalated after Iran's seizure of the British oil tanker in July 2019. Photo by SalamPix/Abaca/Sipa USA/Newscom.

As cyber vulnerabilities proliferate with the expansion of connected devices, wherein security is often forsaken for ease of use, Special Operations Forces (SOF) cannot escape the obvious, massive risk that they are assuming by incorporating emerging technologies into their toolkits. This is especially true in the maritime sector where SOF operates nearshore in littoral zones. As SOF—in support to the U.S. Navy—increasingly operate in these contested maritime environments, they will gradually encounter more hostile actors looking to exploit digital vulnerabilities. As such, this monograph comes at a perfect time as the world becomes more interconnected but also more vulnerable.

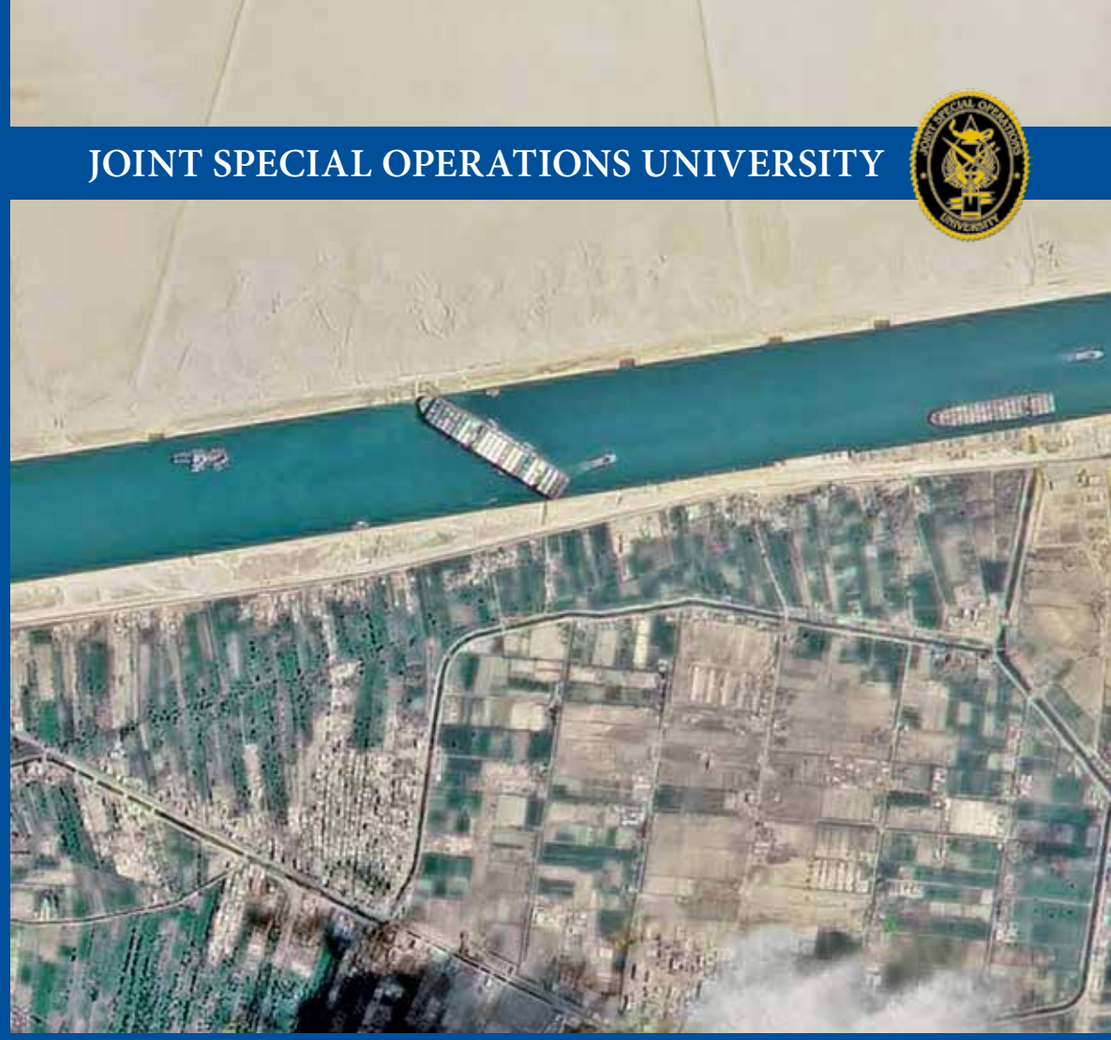
Joint Special Operations University
7701 Tampa Point Boulevard
MacDill AFB, FL 33621

https://jsou.libguides.com/jsoupublications

JOINT SPECIAL OPERATIONS JSOU UNIVERSITY PRESS

ISBN 978-1-941715-55-0

JSOU Report 21-4 Cross Domain IW Threats to SOF Maritime Missions Kessler/Zorri JSOU



JOINT SPECIAL OPERATIONS UNIVERSITY

Cross Domain IW Threats to SOF Maritime Missions: Implications for U.S. SOF

Gary C. Kessler and Diane M. Zorri

JSOU Report 21-4

Joint Special Operations University and the Institute for SOF Strategic Studies (IS3)

The Joint Special Operations University (JSOU) generates, incubates, and propagates (delivers and communicates) ideas, education, and training for expanding and advancing the body of knowledge on joint and combined special operations. JSOU is a 'hybrid organization' that performs a hybrid mission—we are a 'corporate university:' an academic institution serving a professional service enterprise, 'by, with, and through,' the United States Special Operations Command (USSOCOM). As such, we are both a direct reporting unit to the Commander, USSOCOM, on all Combined Joint Special Operations Forces (CJSOF) education and leader development matters, as well as the educational and leader development component of the Command.

The JSOU Mission is that JSOU prepares Special Operations Forces professionals to address strategic and operational challenges, arming them with the ability to think through problems with knowledge and insight. **Our Vision** is to constantly strive to be(come) USSOCOM's "think-do tank," world-class leader in "All Things" CJSOF strategic and operational education, training, and leader development, and the advancement of knowledge on the utility of CJSOF, for the Nation. We pursue this mission and vision through our best-practice teaching & learning, research & analysis (R&A), and engagement & service-outreach operations, activities, and initiatives. We achieve these outcomes-based goals by providing specialized joint professional military education, developing SOF-specific and unique undergraduate, graduate, and post-graduate-level equivalent curriculum, and by fostering special operations-focused R&A and outreach, in support of USSOCOM objectives and United States national and global strategic goals.

JSOU carries forward its R&A roles and responsibilities led by, and through its IS3, where our efforts are guided and informed by the most current U.S. National Security, Defense, and Military Strategies, and the **USSOCOM Mission:** *USSOCOM develops and employs fully capable Special Operations Forces to conduct global special operations and activities as part of the Joint Force to support persistent, networked, and distributed global Combatant Commands operations and campaigns against state and non-state actors, to protect and advance U.S. policies and objectives.*

Joint Special Operations University

JSOU Press publications are available for download at https://jsou.libguides.com/jsoupublications.

Print copies available upon request by writing jsou_research@socom.mil.

Sharpening the Edge of SOF's Advantage: The All-Domain SOF Leader-Professional

Cross Domain IW Threats to SOF Maritime Missions: Implications for U.S. SOF

Gary C. Kessler and Diane M. Zorri

JSOU Report 21-4
The JSOU Press
MacDill Air Force Base, Florida
2021

Recent Publications of the JSOU Press

Cyber Supply Chain Risk Management: Implications for the SOF Future Operating Environment, JSOU Report 21-3, J. Philip Craiger, Laurie Lindamood-Craiger, and Diane Zorri

Mazar-e Sharif: The First Victory of the 21st Century Against Terrorism, JSOU Report 21-2, William Knarr, Mark Nutsch, and Robert Pennington

The Blurred Battlefield: The Perplexing Conflation of Humanitarian and Criminal Law in Contemporary Conflicts, JSOU Report 21-1, Patrick Paterson

Iranian Proxy Groups in Iraq, Syria, and Yemen: A Principal-Agent Comparative Analysis, JSOU Report 20-5, Diane Zorri, Houman Sadri and David Ellis

Special Operations Forces Civil Affairs in Great Power Competition, JSOU Report 20-4, Travis Clemens

Informal Governance as a Force Multiplier in Counterterrorism: Evidence for Burkina Faso, JSOU Report 20-3, Margaret Ariotti and Kevin Fridy

On the cover. Pictured in this image taken from space is the grounded container ship *Ever Given* in the southern section of the Suez Canal. The 400 meter-long container ship, which is registered in Panama, was knocked off course during a sandstorm on 23 March 2021 while en route from China to Rotterdam, Netherlands. The container ship became wedged across the canal, completely blocking the path of other vessels for almost 7 days. Photo by Roscosmos Press Office/TASS/Newscom. Used with permission.

Back cover. Iran's Revolutionary Guard inspect the British-flagged oil tanker *Stena Impero*, which was seized in the Strait of Hormuz by the Guard, in the Iranian port of Bandar Abbas. Tensions in the Persian Gulf escalated after Iran's seizure of the British oil tanker in July 2019. Photo by SalamPix/Abaca/Sipa USA/Newscom. Used with permission.

May 2021.

ISBN 978-1-941715-55-0

The views expressed in this publication are entirely those of the authors and do not necessarily reflect the views, policy, or position of the United States Government, Department of Defense, United States Special Operations Command, or the Joint Special Operations University.

Products or services mentioned in this monograph are for informational or example purposes only, and should not be construed as a recommendation or reference for such products or services.
Any product or company mentioned in reference to a cybersecurity breach or other incident is for completeness only and has already been publicly identified.

Comments about this publication are invited and should be forwarded to the Director, Institute for SOF Strategic Studies, Joint Special Operations University, 7701 Tampa Point Blvd., MacDill AFB, FL 33621.

****

The JSOU Institute for SOF Strategic Studies is currently accepting written works relevant to special operations for potential publication. For more information, please contact the Director, Institute for SOF Strategic Studies at jsou_research@socom.mil. Thank you for your interest in the JSOU Press.

****

Contents

Foreword

In 2021, the world took notice of the frailty of our interdependent supply chain networks. The Suez Canal, which is one of the busiest trade routes in the world, was closed for almost a week due to the massive container ship, *Ever Given*, becoming stuck after a sandstorm caused visibility to plummet. The dirty secret to this episode: the same effect could have been achieved via cyberspace by infiltrating the ship's integrated technological systems. An ill-intentioned hacker could have achieved the same effect by slightly altering data in the ship's navigation systems.

The vulnerability of maritime transportation systems, like that of the overall vulnerability of supply chain networks, has long been a source of concern within the cybersecurity community. As more devices are attached to the internet, and as more actors come online to exploit digital vulnerabilities, discovering gaps in maritime digital security is becoming increasingly common. The recognition of these gaps in cybersecurity led to the December 2020 release of the *National Maritime Cybersecurity Plan* by the White House National Security Council. Although this plan will not instantly solve a long-standing problem, it does streamline federal cybersecurity standards for maritime transportation systems. Here, cyberspace risk hides in plain sight: the opacity of operational technology masks risk, thereby allowing malign actors to exploit networked systems.

As cyber vulnerabilities proliferate with the expansion of connected devices, wherein security is often forsaken for ease of use, Special Operations Forces (SOF) cannot escape the obvious and massive risk they are assuming by incorporating emerging technologies into their toolkits. This is especially true in the maritime sector where SOF operates nearshore in littoral zones (LZ). As SOF—in support of the U.S. Navy irregular warfare (IW) mission—increasingly operate in these contested maritime environments, they will gradually encounter more hostile actors looking to exploit digital vulnerabilities. As such, this monograph comes at a perfect time as the world becomes more interconnected but also more vulnerable.

The monograph's authors, Gary Kessler and Diane Zorri, not only articulate the various vectors of digital compromise but also explicate how various maritime systems work and include real world examples of compromise. The

authors aim to reach a broad audience, not just those involved in the maritime domain. Hence, Kessler and Zorri start each chapter discussing what relationship SOF has to a particular digital tool. They then define what each digital tool is and provide case studies. The authors end each chapter with concluding observations that bring together and summarize the entire chapter. These concluding observations are particularly helpful and quick takeaways for the executive that cannot read the entire monograph.

The authors of this fantastic volume provide the SOF reader with three key takeaways: competitive advantage, maritime IW, and technology vulnerabilities. Readers will agree that these takeaways ultimately provide both opportunities and risks for SOF, and that by confronting these takeaways early, SOF will be better positioned to compete globally in the future.

Cybersecurity vulnerabilities will not go away. Therefore, it is up to SOF to reduce the magnitude of its own digital vulnerabilities while exploiting the vulnerabilities of its adversaries. Reading this monograph is a good place to start on understanding just how SOF can achieve that objective.

Mark G. Grzegorzewski, Ph.D.
Professor, Institute for SOF Strategic Studies

About the Authors

Dr. Gary Kessler, CISSP, is a principal consultant at Fathom5 and president of Gary Kessler Associates in Ormond Beach, Florida, providing consulting, research, and training related to maritime cybersecurity and network protocols. He is the co-author of the recently published *Maritime Cybersecurity: A Guide for Leaders and Managers*. Gary is a retired professor of cybersecurity from Embry-Riddle Aeronautical University in Daytona Beach, Florida. He was visiting faculty at the U.S. Coast Guard (USCG) Academy in the fall semester of 2019, where he still gives talks about maritime cybersecurity. Gary holds a bachelor's degree in mathematics, a master's degree in computer science, and a Ph.D. in computing technology in education. He has been involved in the information security field since the late 1970s; his latest research efforts have been related to Automatic Identification System (AIS) security. He is a member of the USCG Auxiliary, where he is the Chief of the Cyber Augmentation Branch of the Cybersecurity Division. Gary is active in National Marine Electronics Association (NMEA) standards development, is a scuba instructor and holds a 50 Gross Ton merchant mariner credential. More information can be found at https://www.garykessler.net.

Dr. Diane Maye Zorri is an Assistant Professor of Security Studies at Embry-Riddle Aeronautical University in Daytona Beach, Florida and a non-resident Senior Fellow with Joint Special Operations University. Prior to Embry-Riddle, Dr. Zorri served as a visiting professor at John Cabot University, in Rome, Italy and as an affiliated scholar with George Mason's School for Conflict Analysis and Resolution. Prior to her work in academia, she was an officer in the United States Air Force and later worked in the defense industry doing foreign military sales, integrated communications, and proposal development for an Italian defense conglomerate. She is a graduate of the U.S. Air Force Academy, Naval Postgraduate School, and earned a Ph.D. in political science from George Mason University's Schar School of Policy and Government.

Acknowledgements

The authors would like to thank JSOU project manager Mark Grzegorzewski, reviewers Dave Ellis and Pete McCabe, and the entire JSOU editorial and support team as they guided us through the process of creating this paper.

Introduction

> A ship in harbor is safe, but that is not what ships are built for.
> - John A. Shedd[1]

United States Special Operations Command (USSOCOM) has identified several emerging threats to U.S. Special Operations Forces (SOF). These include, but are not limited to strategic sabotage, vulnerability to missile attacks, and innovative uses of technology by state and non-state competitors.[2] These threats highlight the importance for Special Operations Forces (SOF) to maintain the competitive advantage in support of U.S. Navy irregular warfare (IW), especially across globally contested domains, such as coastal and near-coastal environments.

If the threats above can be viewed as independent "vertical" vectors, the cybersecurity threat vector would be the "horizontal" that ties them together. Cyber and other electronic threats particularly in the maritime domain, have grown dramatically over the last decade. More and more actors are using cyber threats as a line of effort against U.S. naval forces and their components. Malign actors understand that the maritime realm depends upon automation, and they seek to exploit vulnerabilities in shipboard systems. While there is appropriate concern being given to traditional great power adversaries—e.g., China, Russia, and Iran—tactical and strategic sabotage on information and information-dependent systems are becoming so commonplace and inexpensive that smaller nation-state adversaries and organized groups can take advantage of this deficiency by acting on their own or as proxies for great powers. Coupled with the relative ease with which information can be weaponized with fairly insecure maritime systems, and we see a formula for a new form of IW. This form of IW is exacerbated when we look at the littoral, or nearshore zone (LZ) of the world, since the biggest physical threats to ships are in the relatively shallow waters of the coast and inland waters.

Overview

This report will explore and identify maritime cyber threats that promote or enable IW vectors that can negatively impact naval activities within the scope

of USSOCOM. Moreover, this monograph integrates both the maritime and the cyber domains of warfare. While the intersection of the maritime environment and the cyber realm is not explicitly defined, the U.S. Department of Defense (DOD) describes operations in cyberspace as follows:

> Most aspects of joint operations rely in part on cyberspace, the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. Developments in cyberspace provide the means for the U.S. military, its allies, and partner nations to gain and maintain a strategic, continuing advantage in the operational environment (OE).[3]

There are many ways in which sub-state actors, jihadists, and other terrorist organizations are waging a guerrilla war on the sea via cyberspace.[4] Increasingly sophisticated and damaging cyberattacks are becoming more commonplace everywhere. Furthermore, attacks in cyberspace are now relatively easy and inexpensive, including the jamming and spoofing of navigation messages to cause confusion or misdirection in and around ports.[5] If an adversary cannot manage a cyberattack on its own, it can ally with like-minded hacking groups—or, hire such a capability from those who advertise "hacking as a service." Hacking groups from China—such as APT10 and TEMP.Periscope—have targeted the maritime industry, U.S. Defense Industrial Base (DIB), and U.S. military assets abroad.[6] As noted in a 2019 audit by the Office of the Secretary of the Navy, both commercial and government maritime systems have become increasing susceptible to cyberattacks.[7] It has manifested as a global grey zone conflict, where proxies and cyber mercenaries use non-kinetic means to intimidate adversaries, steal precious defense technology, and compromise data and control systems. Thus, the most dangerous part of a sea voyage is often not in the deep ocean, but in the shallow waters of the LZ—including inland waters and ports—where malign actors can infiltrate a ship's integrated technological systems. Causing a ship to veer from a precise course by even a few tens of meters can cause significant damage to vessels, ground assets, and/or delay vessel and cargo transport. Small errors in tight waterways ripple quickly and can rapidly lead to progressively more damaging second-, third-, and fourth-order effects.

Characteristics of the LZ

The LZ refers to near coastal waters—the area of the ocean most affected by tides and currents, shallow waters, and vagaries of a coastline. This is the part of the ocean where local mariners would have the most intimate knowledge, a distinct advantage over transient sailors and guests. In hostile regions around the globe, the zone is often most traversed by seafarers without the means or reach of deep-sea watercraft. Water conditions change several times a day, as well as seasonally; small errors in navigation can cause disastrous results, being the difference between open water and running up on rocks.[8] This section will describe the characteristics of the LZ and considerations related to IW.[9] For this discussion, we will use the DOD definition for littoral:

> The littoral comprises two segments of operational environment: 1. Seaward: the area from the open ocean to the shore, which must be controlled to support operations ashore. 2. Landward: the area inland from the shore that can be supported and defended directly from the sea.[10]

The LZ, then, is the area where tides and currents are a significant factor on both water movement that affects ships and erosion that affects a changing seabed and shoreline. This is the area where the power and energy of the ocean is most acutely felt.[11] While the water is often the focus of the LZ, much of the understanding of the near coastal sea is dependent upon understanding the shoreline and the interactions between the near coastal landscape and the water.[12] See Appendix A for a more detailed description.

More significantly, the LZ has grown in its political, logistic, demographic, and economic importance over the past three decades. After the fall of the Soviet Union and the collapse of the bipolar world order, tensions between states seeking regional hegemony—such as Iran and Saudi Arabia—have proliferated. The threat is most critical in strategic maritime chokepoints such as the Strait of Hormuz—where up to 21 million barrels of crude pass each day[13]—or the Bab el-Mandeb Strait, which lies at the intersection of the Red Sea, Horn of Africa, and the Indian Ocean. Similarly, the vast majority of the world's capital cities and population centers are in the littorals, underscoring their logistic and economic enormity.[14]

Because the LZ is where the sea and the land meet, straits and ports are in this zone and represent chokepoints for both merchant and military vessels.

Nearly 40 percent of the world's population lives within 60 miles (100 kilometers) of the coast, and almost three-quarters live within 200 miles (320 kilometers) of the coast. It is also noteworthy that nearly 600 million people live in coastal areas at an elevation of less than 33 feet (10 meters) above sea level. Indeed, sea level rise presents a tactical issue as it impacts coastal erosion, storm surges, and tidal water encroachment into estuaries and near-coast river systems. Climate change has a disproportionate impact on the LZ compared with inland communities.[15]

Nearly 40 percent of the world's population lives within 60 miles (100 kilometers) of the coast, and almost three-quarters live within 200 miles (320 kilometers) of the coast.

Operating a vessel in the LZ requires a different skill set than operating on the open ocean. For instance, pilots are needed in complex harbors and inlets because of the requirement of local knowledge for safe passage. Navigability of near-coastal waters depends on tides (and whether they are diurnal vs. semi-diurnal[16]), currents, and weather. Shoaling within a channel or river can quickly change the nature of the passage. Pilots need accurate charts to indicate the bottom composition, hazards to navigation, and other landmarks to aid positioning. Small, unanticipated changes in geographic position can be fatal to a vessel; accurate knowledge of location is important. Understanding the tidal effects on vessels, in terms of both water depth and current, are imperative. A small tidal change of just a few feet (1 meter) can cause ripping currents in some areas, while tidal bores of 5–30 feet (1.5–9 meters) occur in other regions; extreme tidal ranges of more than 50 feet (15 meters) are seen in the Bay of Fundy and Leaf Basin in Ungava Bay, Canada.[17]

The LZ is such a unique place in terms of military operations that the U.S. Navy designated a new class of surface warfare vessel in 2002 known as littoral combat ships (LCS). Because they are designed specifically to operate in the LZ, they take advantage of the fact that many traditional shipboard functions such as training, some maintenance, and logistics, can actually be performed on shore—thus reducing crew size and allowing for ships to be specifically designed to the nearshore task.[18] These specialized craft can be more rapidly constructed at a lower cost than traditional Navy warships, meaning that more can be produced in order to focus on the asymmetric threats of IW in this zone.[19]

SOF in the LZ

Historically, SOF has been extremely active in the LZ. Operations inside the littorals include raids; ambushes; combat swimmer attacks; sabotage; abductions; reconnaissance; harbor penetration; visit, board, search and seizure; and extractions. Yet, as the U.S. military postures itself for an era of great power competition, some have questioned the utility of the LCS.[20] Meanwhile, the 21st century has seen the near coastal waters become the most active setting for discord in the maritime domain. Instead of major sea battles between large ships, the fight is in the domain of "irregular" adversaries, especially as smaller forces act as proxies for larger nation-states and near-peer competitors.[21] Engagements with irregular forces and non-state combat at low intensities has shown an upward trend, thereby creating the need for SOF to become increasingly prepared to engage and preempt the tactics of adversaries in the LZ.[22]

Cybersecurity in the LZ

Although relatively well understood at a strategic level, little has been discussed about the cybersecurity impacts on warfare in the LZ.[23] Like so many other aspects of applications of technology, cybersecurity implications are often an afterthought rather than considered during design and planning. Indeed, ship design and planning evolves at a much slower rate than changes in the cybersecurity threat landscape, making it difficult for ship infrastructure to keep up with cyber in the best of circumstances. Cybersecurity in the maritime domain has only become a focus area in the last decade and impacts many aspects of the operation of the entire Maritime Transportation System (MTS). The remainder of this document will specifically address several aspects of maritime cybersecurity as it impacts vessels in the LZ and cyberattacks that might be employed by irregular adversaries.[24] Much of the discussion will cover implications for civilian vessels but might be equally applicable to—or could have an impact upon—military vessels. The nature of the LZ is such that civilian vessels will always be a factor because of their presence, relative ease of exploitation, and potential to become a threat to SOF operation. In addition, irregular adversaries might view civilian vessels as a target for hostile activity, cover for hostile activity, or as a weapon to use against traditional military forces.[25]

Key Takeaways

This monograph presents three key takeaways:

1. **Competitive Advantage.** USSOCOM's agility, global presence, and combat-focused mission requires forward thinking preparation and planning. As a combatant command that is joint by nature, USSOCOM is uniquely postured to maintain the competitive advantage in cross-domain operations, such as maritime cyber.
2. **Maritime IW.** The maritime domain enables U.S. global reach and global power. While great power competitors and near-peer adversaries are growing their conventional forces, they are also pushing back against U.S. interests though proxies and gray-zone activities, especially in the maritime domain. SOF support of U.S. Navy IW is central towards limiting the maneuver capability of hostile forces.
3. **Technology Vulnerabilities.** While advances in the integration of maritime, satellite, and cyber technologies have greatly enabled the U.S. armed forces, nefarious activities such as hacking and spoofing are on the rise, enterprise-level maritime systems are vulnerable, and malign actors have been able to penetrate various points in the global supply chain. It is incumbent upon the SOF community to recognize these challenges, develop plans to test the resiliency of the force, and counter hostile actors when necessary.

Organization of This Monograph

This monograph addresses how threats in cyberspace can negatively impact maritime U.S. SOF operations in littoral waters. The objective of this report is to identify relevant maritime cyber vulnerabilities that can be exploited and turned into viable threats against U.S. SOF. The relative risks of these vulnerabilities are also assessed and ranked to provide a strategy of how to mitigate, combat, or otherwise manage the dangers; thereby supporting the U.S. Navy's intent of maintaining maritime superiority.

This section has provided an overview of the characteristics of the LZ and the relationship of that region to IW. Subsequent sections describe the most salient cybersecurity vulnerabilities in the maritime domain and their impact on warfare in the LZ. Chapter 1 reviews global navigation satellite

systems (GNSS) and the implications of electronic attacks on positioning, navigation, and timing (PNT). Chapter 2 examines the automatic identification system (AIS) and vulnerabilities that can lead to numerous attacks affecting vessel situational awareness. Chapter 3 discusses how viruses, worms, and other malware can impact maritime systems, and how SOF can organize to be more resilient against vulnerabilities in the defense supply chain. Chapter 4 introduces how cyber vulnerabilities in industrial control systems (ICS) and Internet of Things (IoT) devices can lead to problems aboard ships and at ports. Chapter 5 discusses autonomous vessels and the ramifications of cyber vulnerabilities. The final chapter presents conclusions and the implications of maritime cyber issues for SOF, and the role of SOF in defense of U.S. Navy assets. The appendices provide technical background detail to the topics above so that the interested reader can further extrapolate their impact on IW.

Chapter 1. Global Navigation Satellite Systems (GNSS)

> A poor grasp of dead reckoning may have led Christopher Columbus to North America instead of India, a navigational error of about 8,000 miles. - Eric Schlosser[26]

Humans have been navigating on the high seas for several thousand years. Early mariners used the weather, nature of the seas, position of stars, and presence or absence of certain bird and fish species to navigate from one place to another.[27] The astrolabe, likely developed as early as the second century to determine latitude, was not routinely used until the 1400s by European explorers.[28] The first circumnavigation of the globe using charts and instruments was reportedly accomplished by Magellan around 1520. Accurate marine chronometers with which to determine longitude were not available until the late 1700s.[29] Maritime navigation aided by radio was developed in the early 1900s, followed by radar navigation in the mid-1900s, and satellite navigation in the late 1900s.[30]

GNSS refers to the myriad systems employing this latest generation of navigational aid. GNSS can also refer to the software applications that work with the Global Positioning System (GPS), such as target acquisition, missile guidance, search and rescue (SAR), coordinate bombing, precision survey, instrument approach, range instrumentation, close air support, surveillance, and reconnaissance. Although professional mariners rely on much more than just electronic aids for navigation and plotting, there is still considerable reliance on technical solutions and many still trust the electronics more than their own senses when the two are in conflict. This section will discuss some background of GNSS and GPS, and potential cybersecurity vulnerabilities that can cause particular hazards in the LZ. Technical details about the operation of GNSS and GPS systems can be found in Appendix 2.

SOF and GNSS

Attacks on GNSS might generally be considered as falling more under the category of electronic warfare (EW) rather than cyberwarfare. The DOD

recognizes that many cyberspace operations include traditional computer- and network-based attacks on data, as well as significant portions of EW and other mission areas.[31] Indeed, software-defined radio (SDR) for wireless networks and other emerging technologies are blurring the line between the common understanding of cyberattacks and EW, and these two missions are falling closer into alignment.[32]

Rather than employ the term *secure* GPS, DOD instead uses the term PNT, thereby both encapsulating the vulnerabilities of GNSS and the expectations of the users.[33] DOD has even defined the term *navigation warfare* to refer to defensive and offensive operations that affect PNT capabilities.[34] Meanwhile, GNSS applications are of particular relevance to the SOF community. GNSS technologies such as anti-jam GPS, anti-spoofing software, and EW systems allow SOF to operate in denied areas.[35] USSOCOM reported that "2017 and 2018 saw unprecedented GNSS interference activity, from the eastern Mediterranean to Norway and Finland."[36] GNSS interference, and particularly GPS spoofing, which causes the receiver to give false information, can mean the difference between life and death in military contexts. These technologies have become more affordable and widely available, putting the SOF community in unprecedented danger.

GNSS interference, and particularly GPS spoofing, which causes the receiver to give false information, can mean the difference between life and death in military contexts.

GNSS Overview

GNSS is a generic term that refers to the four global satellite navigation systems: China's BeiDou; Galileo, created by the European Union (EU); Russia's Global Navigation Satellite System (GLONASS);[37] and the U.S. GPS—plus the two regional systems: India's Navigation with Indian Constellation (NAVIC)[38] and Japan's Quasi-Zenith Satellite System.[39] Each of these systems are independent of one another, but work in a similar fashion. For purposes of this report, GPS will be the primary focus.[40]

Originally named NAVSTAR, GPS began as a joint project of the U.S. Air Force and U.S. Navy in the late 1960s and is generally considered to be the first GNSS. The GPS system and satellite constellation are currently managed by the U.S. Space Force.[41] GPS transmits messages on three frequencies in

the L band (1–2 GHz), denoted L1, L2, and L5.[42] Each message contains such information as the current date and time, exact position of the transmitting satellite, and an approximate position of every satellite in the constellation. A GPS receiver can determine its exact geographic position by acquiring the signal from four satellites; the fourth satellite is essential for the recovery of the clock, which can reduce positioning error to just a few feet (1 meter).[43]

GPS satellites transmit their navigation messages in both encrypted and unencrypted form. The unencrypted messages are freely available to the public for civilian use and standard precision applications. The encrypted messages are intended for military and other official applications, making the signals more robust and resistant to spoofing than civilian GPS.[44]

GNSS Security Vulnerabilities and Mitigations

GNSS technologies have been under development since before the 1970s. With the exception of the use of encrypted codes for military applications, security was not one of the design criteria. Although GPS and other GNSS are undergoing constant upgrades and improvements in their technology, protocols, clocks, and extended satellite lifetimes—a process often referred to as GNSS Modernization—the systems remain vulnerable to several types of deliberate attacks that modernization does not address; of particular relevance to maritime operations in the LZ are jamming, spoofing, and timing signal attacks.[45]

Jamming

GNSS jamming refers to any device or method intended to interfere with the GNSS satellite signals. Jammers work by distorting or otherwise overpowering the signal so that the receiver cannot obtain its navigational fix. Since the GNSS signal reaches the surface at an extremely low power level, a small transmitter in the same frequency range can overpower the legitimate GNSS signals. Jammers are inexpensive and easy to purchase or build; a jammer for "personal use" the size of a hand-held radio can cause localized jamming within a 165 foot (50 meter) radius for a cost of about $150[46] and a more sophisticated jammer to cause a more widespread outage is well within the financial reach of an adversarial force.[47]

Jamming can be very effectively used by one military force against another, because different GNSS constellations use different frequencies

(table 1). Thus, if two opposing forces are using different GNSS systems, one can safely jam the signals of the other without impacting their own signals.[48]

Table 1. L band frequencies used by GNSS with global coverage. Source: Lavrov, Russia's GLONASS Satellite Constellation

BeiDou	Galileo	GLONASS	GPS
1561.098 MHz (B1) 1207.140 MHz (B2) 1268.520 MHz (B3)	1575.42 MHz (E1) 1176.45 MHz (E5a) 1207.14 MHz (E5b) 1278.75 MHz (E6)	1602.0 MHz (L1) 1246.0 MHz (L2) 1202.0 MHz (L3)	1575.42 MHz (L1) 1227.60 MHz (L2) 1176.45 MHz (L5)

Another technology that allows easy access to advanced jamming is SDR. SDR uses a hardware transmitter that plugs into a computer's Universal Serial Bus (USB) port, an external antenna, and freely available, open-source software in order to transmit any desired signal on any frequency the transmitter/antenna are capable of, including those in the ultra high frequency (UHF) L-band. Use of SDR transmitters are within the technological reach of almost anyone, and there are even YouTube videos providing tutorials for building such devices.[49]

It is relatively straight-forward for GNSS receivers to detect efforts at jamming; analysis of the frequency power spectrum or measuring the signal-to-noise ratio can indicate interference.[50] Many GPS receivers, in fact, have built-in jamming—and spoofing—detection. Low-cost jamming detection can even be built using SDR, the same inexpensive "do it yourself" technology that can be employed to build a low-cost jammer.[51]

While GNSS jamming is possible to detect and track—even from space[52]—there are very few good defenses against deliberate jamming of GNSS signals. If a jamming signal is primarily interfering from a single direction, an anti-jamming antenna can be used to alter the gain to essentially ignore the jamming signal and rely on other legitimate signals. If several jammers can target a receiver from multiple directions, the only defense might be to employ a different GNSS constellation. The lesson here is that any allied military operation would be well served to use receivers that employ at least Galileo and GPS; utilization of multiple constellations provides both redundancy in case one system fails and the capability to ensure positional integrity by cross-checking between different systems.[53]

Spoofing

GNSS spoofing, as opposed to jamming, refers to actions that cause a receiver to lock on to a bogus signal and miscalculate its position. Unlike jamming, where a false signal merely needs to overwhelm a legitimate one, a spoofed transmission needs to have the same structure and timing as a legitimate GNSS navigation message, but changed in such a way that the receiver miscalculates its location.[54] Because of the use of encrypted ranging codes, military GNSS units are largely immune to spoofing unless the decryption keys are compromised;[55] they are not immune, however, to jamming.

GNSS spoofing is always a deliberate act; it is complex and requires specialized equipment that can disrupt a legitimate signal in order that the victim computes a false position fix and/or a false clock offset.[56] Most spoofing methods require that the bogus transmitter overwhelm the satellite signals being received by a GNSS device and therein lies one of the ways in which spoofing can be detected. First, when the GNSS receiver locks on to the bogus signal, there is a distortion as it loses the legitimate signal, resulting in a blip that is visible on the GNSS display; there is no such distortion when there is a handoff between legitimate satellites (or if the spoofing device slowly increases its power so as to appear like a normal handoff). This anomaly can be seen in figure 1. In this example, after successful spoofing the GPS signal, attackers prompt the helmsman to steer the vessel off its original course (upper graph). The individual codes emitted by a half-dozen GPS satellites disappear at about the 400-second mark, as the spoofer captures the ship's receivers (middle graph). Second, a spoofing detector based on monitoring the signal's direction-of-arrival could warn the crew when it senses too little variance in the origins of the signals, as seen here at the 400-second mark (lower graph).[57] Legitimate GNSS signals will come from at least four different satellites which are in four different directions (and distances) relative to the receiver whereas a spoofer can, presumably, only be in one place at one time so all signals will appear to come from the same direction and have the same relative power when received.[58]

GNSS spoofing is always a deliberate act; it is complex and requires specialized equipment that can disrupt a legitimate signal in order that the victim computes a false position fix and/or a false clock offset.

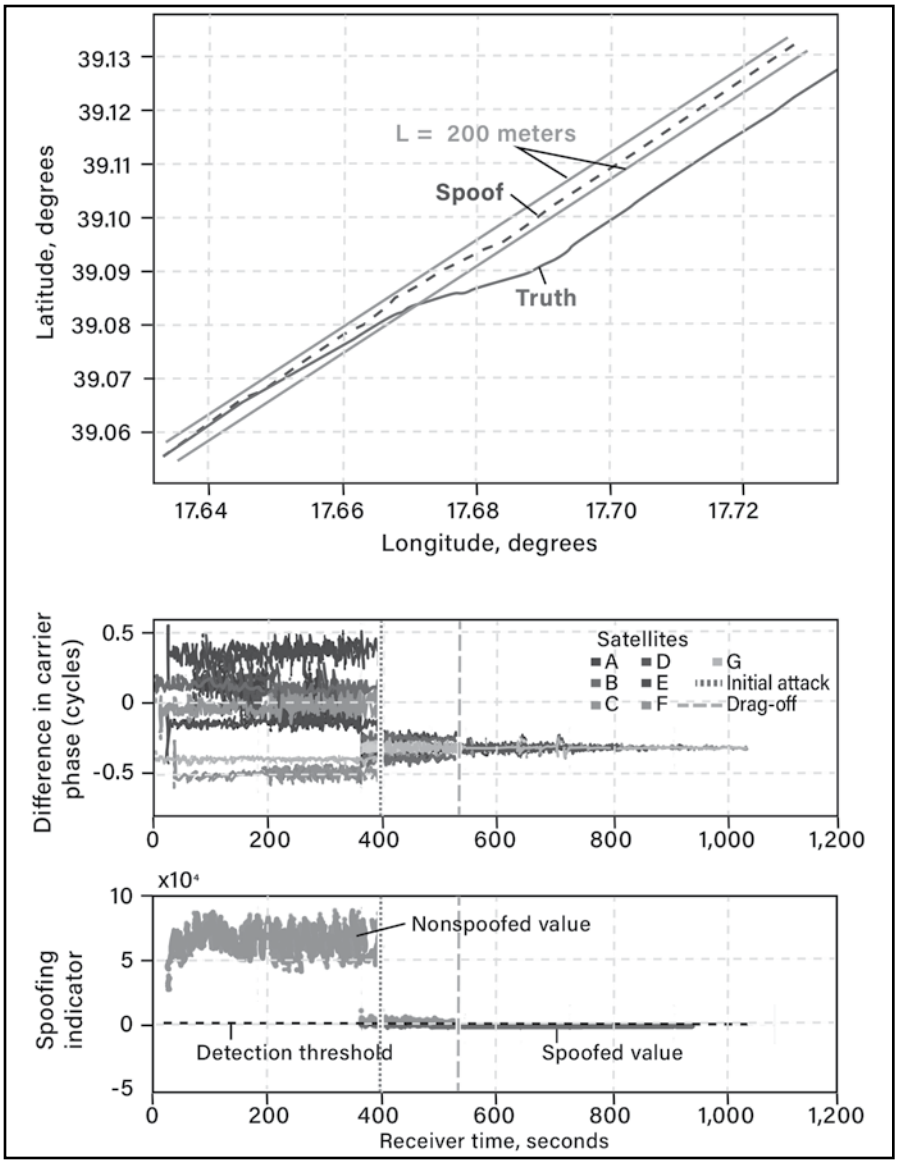


Figure 1. Anomalies appear during a GPS spoofing attack.
Source: Todd Humphreys/used with permission

There are several detection methods or workarounds to GNSS spoofing. Two methods are mentioned above: signal distortion detection, and direction-of-signal detection. A third method correlates the encrypted code on the L1 channel with the unencrypted code to ensure authenticity—even though a civilian GPS receiver cannot read the encrypted code information.[59] Another defense for civilian GNSS units, as with jamming, is to employ receivers that can employ multiple constellations; when spoofing is detected, the receiver can change to another constellation.[60]

One reason civilian receivers are more vulnerable to spoofing is only partially related to the use of encrypted codes; military devices are also hardened because the encrypted code acts as a mechanism to authenticate the transmitter. If a civilian GPS unit receives properly formatted unencrypted signals, the device has no way to know if those signals are legitimate or spoofed. While many of these types of attacks are unlikely from "irregular" warriors, they are well within the capabilities of a nation-state that sponsors irregulars as proxies.

Other GNSS Vulnerabilities

A third major form of attack on GNSS systems is to disrupt the timing signal. GNSS-derived timing affects more than GNSS receivers. Many systems rely on GNSS to obtain their time; all digital telecommunications systems, including the North American mobile phone network and digital telecommunications carriers, must be synchronized to operate properly. Power grids and some Network Time Protocol servers on the internet also derive timing from GPS. Any system relying on GPS positioning—such as Enhanced 911 (emergency) triangulation, or aviation and maritime transportation systems—requires precise timing.[61] Timing disruptions do not need to be large to have big effects; a 1 nanosecond (10^{-9} second) error in timing can cause a 1 foot (30 centimeter) positioning error.[62] Again, this form of disruption is beyond the means of irregular warriors but not their nation-state sponsors.

A variety of mitigations have been suggested to deal with timing attacks, all essentially providing backup or augmentation to a device's dependence upon GNSS for synchronization. One approach is to employ inertial navigation systems and inertial measurement units (IMU). IMUs use a combination of sensors, accelerometers, and gyroscopes to independently measure movement without use of an external reference, essentially employing a

highly advanced form of dead reckoning.[63] Other approaches include proposals to build alternate timing systems to provide an external reference for GPS.[64] Finally, radio signals do not need to be manipulated to send bogus GNSS information if an adversary can gain physical access to a vessel. Such physical access to a military vessel is unlikely but manipulating civilian or autonomous vessels in the LZ can also serve an adversary's purpose.

Messages can be sent between onboard devices requiring GNSS data via a variety of communications interfaces, such as the serial port (e.g., EIA-RS-232), USB, Bluetooth, Wi-Fi, SDR, and UHF radio.[65] If bogus GNSS messages can be introduced into the system from one compromised device, the result can be false GNSS displays, operational errors, or, at the very least, confusion as to accurate position.[66]

GPS Disruption Case Studies and Implications

Jamming and spoofing of GNSS signals have grown so significantly since 2010 that it has become a strategic weapon of conflict.[67] It is certainly a major threat to commercial shipping and that can very well translate to a warzone which, by its nature, is intermixed with commercial and other civilian vessels.[68]

Instances of GNSS jamming have become commonplace in the news. Although illegal in the U.S. and many other countries, GNSS jammers are routinely used by many people under the guise of protecting their privacy. In one case, a man in New Jersey used a GPS jammer so that his employer would not know where he was during his breaks. His route took him near Newark Liberty Airport, and he inadvertently jammed the airport's GPS system during trials of its automatic aircraft landing systems.[69] While his intent was personal privacy, a nefarious user or an adversary could certainly use these same devices at any time. And, as mentioned above, jammers are relatively simple to build and easy to acquire.[70] In many ways, jamming is the most significant problem facing GNSS since it has a low cost of entry, employs off-the-shelf technology, and can impact both civilian and military receivers.[71]

The first widely publicized civilian GPS spoofing demonstration of capability occurred in 2013. In this incident, a team from The University of Texas at Austin (UT) spoofed GPS signals in the Mediterranean Sea, causing *White Rose Of Drachs*, a 213 foot (65 meter) yacht, to alter its course and heading.[72]

So much has been written about this event that any malicious actor could use it as a blueprint for how to carry out such an attack. The team used commercial, off-the-shelf products rather than sophisticated specialized equipment, making it particularly relevant to an irregular adversary.

The first step in the spoofing operation was for the UT team to determine which GPS satellites would be visible to the target at a given time. Using publicly available databases, the team fabricated the unencrypted codes on the L1 band for each visible satellite. At that point, the spoofing device started to broadcast very low-power signals carrying the legitimate codes of all the visible satellites. The spoofer slowly increased the power of the bogus signal until, eventually, the receiver latched onto the new signal and lost the legitimate signals. By increasing the false signal strength slowly, the likelihood decreases of the receiver or the ship's crew detecting a blip. Once the GPS receiver is listening to the bogus signals, the spoofing device can send a new set of position coordinates. In this case, the UT team sent signals that made it appear that the vessel had drifted three degrees to the left, a shift so slight that the crew assumed it was due to natural winds and currents. The crew then compensated for this by shifting the vessel slightly to the right which, in fact, took them off course. The test was terminated after *White Rose Of Drachs* was brought about 3,300 feet (1 kilometer) off course. While the crew had *a priori* knowledge that an attack would take place, they had no specific knowledge about how the test would be conducted nor did they knowingly cooperate with the attack team. Furthermore, a navigation system would have responded the same as the crew—albeit more quickly—so this same spoofing attack would have worked against a vessel using an autopilot.[73]

The UT demonstration of capability became an alarming reality in 2017 when a mass GPS spoofing event occurred in the Black Sea. On 22 June 2017, the master of the 37,500 ton tanker *Atria*, off the Russian port of Novorossiysk, reported that his GPS showed *Atria* to be at Gelendzhik Airport—20 nautical miles (37 kilometer) away (figure 2). Navigation systems from at least 20 nearby ships showed them all to be at the same location, so closest point of approach (CPA) alarms on many vessels were indicating imminent collisions.[74]

At the time of the Black Sea incident, there was widespread speculation that it was due to Russian EW. According to a 2019 report from the Center for Advanced Defense Studies (C4ADS), the Black Sea event was, in fact, part of a larger pattern of Russian GNSS interference. By analyzing satellite data

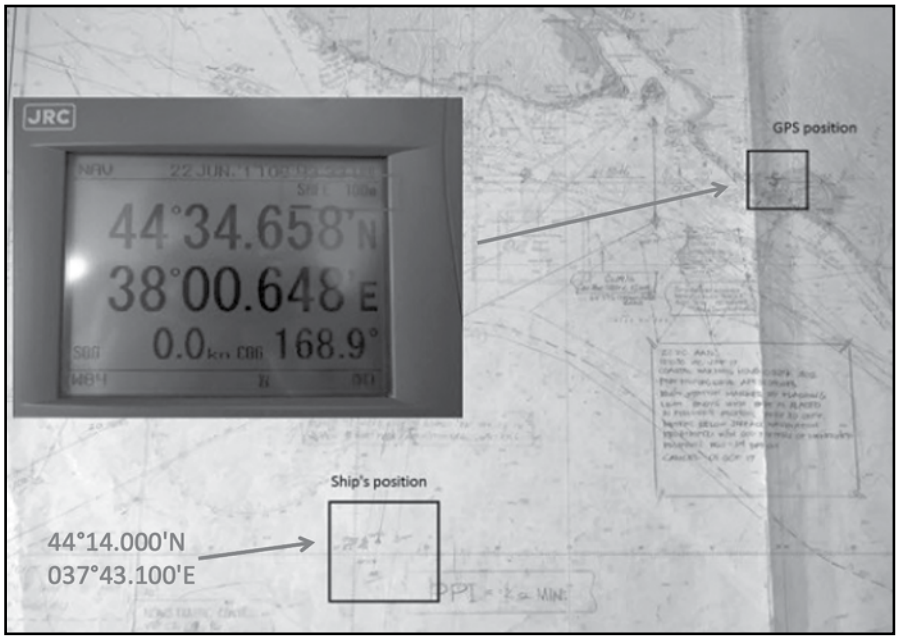


Figure 2. A GPS display on board the *Atria* during a spoofing event shows reported versus actual position. Source: Captain Gurvan Le Meur/used with permission

gathered by the International Space Station (ISS), C4ADS concluded that Russia has been manipulating civilian GNSS signals since at least 2016. The ISS data show nearly 9,900 suspected spoofing incidents associated with the Russian military at ten global locations, including the Black Sea, Crimea, the Russian Federation, and Syria. The data also show more than 1,300 civilian vessels fed incorrect positional coordinates from a range of civilian satellite networks, including the 2017 incident reported by *Atria*.[75]

Since 2018, there have been many reports of GNSS issues in the Eastern Mediterranean, including signal interference, reduced position accuracy, and loss of signal.[76] The affected areas ranged from Cyprus and the coast of Egypt to Israel and Saudi Arabia, resulting in multiple maritime advisories from the U.S. Coast Guard (USCG) and the U.S. Maritime Administration.[77] GNSS outages continue to be a common occurrence all over the world impacting merchant shipping and other mariners.[78] GPS spoofing incidents in Russian waters are also continuing, and have placed ships at multiple airports—including Sochi, St. Petersburg, and Vladivostok.[79]

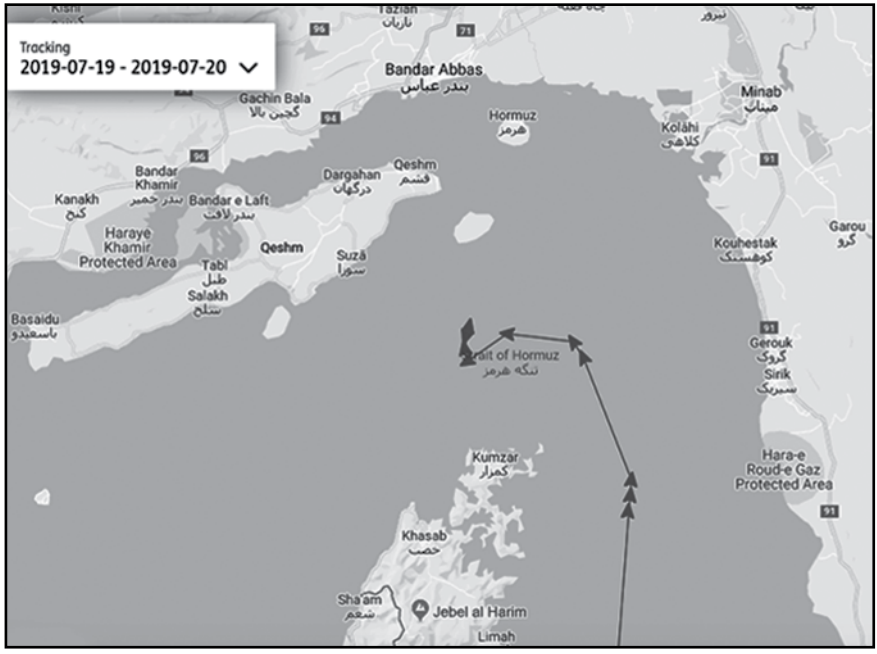


Figure 3. The reported track is shown of *Stena Impero* just prior to its seizure by the Iranian Navy. Source: Lloyd's List Intelligence/used with permission

In July 2019, an escalation in the weaponization of GNSS spoofing reportedly occurred in the Strait of Hormuz. *Stena Impero*, a United Kingdom (UK)-flagged oil tanker, was seized by Iran ostensibly for violating international law. One claim was that it collided with a fishing boat, and another was that it was in the wrong channel when exiting the Strait. Regardless of the stated reason, reports had already come out that Iran was using GNSS spoofing, and a satellite track of the vessel shows it making a normal pass through the Strait before taking a sudden veer towards Iranian territorial waters (figure 3). Despite their claims of territorial violations, it is widely believed that Iran seized the vessel as retaliation for the British impounding an Iranian-controlled oil tanker earlier in the month in Gibraltar for violating EU sanctions.[80]

A new escalation in GNSS spoofing was found after a reported incident in the Port of Shanghai in 2019. In mid-July, *Manukai*, a 700 foot (213 meter) container ship, was making way towards her assigned berth. While in the Huangpu River, the master of the vessel reported that the navigation system displayed another ship moving in the same channel. Then, the other ship

suddenly disappeared from the navigation screen. After a minute or two, the other ship reappeared, now at the dock. Later, the pattern repeated with the other ship appearing on the display moving in the channel, disappearing, and then reappearing back at the dock. Using binoculars, the master was able to locate the other vessel and confirm that it had never left the dock. As *Manukai* reached its own berth, its GPS receivers and all navigation systems suddenly failed, and the captain was unable to get a fix.[81]

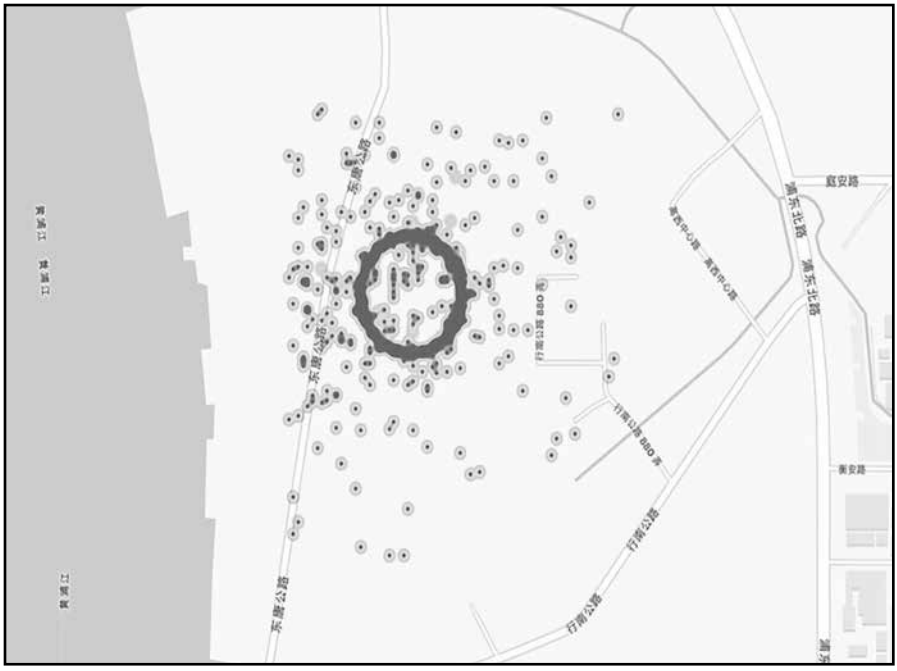


Figure 4. GPS circle spoofing is shown in the area of the Huangpu River near the Port of Shanghai. Source: C4ADS/used with permission

This incident turned out to be just the tip of iceberg. Further analysis of AIS data by C4ADS showed that similar GPS spoofing had been occurring in the area since the summer of 2018—increasing in intensity and number of spoofing incidents over time, hitting a peak of nearly 300 spoofing events on the day that *Manukai* was affected. This event was a major escalation from the previously reported Russian spoofing where all targeted vessels showed up together at a single point; spoofed ships in Shanghai, China were found to jump around every few minutes to different locations that seemed

to concentrate in large circles, primarily on the east bank of the Huangpu (figure 4). Huangpu Maritime Safety Administration (MSA) vessels were among those targeted, where the data show almost daily spoofing attacks; one MSA boat was shown to have been spoofed 394 times in a nine month period.[82] This so-called *circle spoofing* has also been reported in Iran and in other locations around the world, where vessels have found their equipment reporting their location thousands of miles from their actual position.[83] By all appearances, GPS spoofing is a part of an escalating maritime electronic war in the area of Shanghai; more on this in the section about AIS spoofing below.

Concluding Observations

This section has described the operation of GNSS, with a particular focus on GPS. Like so many of our technology systems, they are surprisingly fragile and subject to malign intent. The importance of GPS to the nation's critical infrastructures is so acute that an executive order (EO) was issued in early 2020 to identify all ways in which GPS affects our nation's infrastructures and add resiliency to the system.[84] In addition, the USCG—responding to the request of more than a dozen maritime organizations—filed a formal protest with the United Nations over the threat to safe navigation posed by GNSS disruptions.[85]

For the SOF community, GNSS is essential for everyday operations. GNSS provides the warfighter with enhanced situational awareness, terrain awareness, the projection of radio frequency countermeasures, and the ability to operate in denied environments. The GNSS-enabled warfighter is autonomous and—when it comes to understanding location, even in those hostile and foreign—largely self-sufficient. Without GNSS, the warfighter becomes more isolated; some communications become increasingly difficult. This kind of disruption can easily paralyze the warfighter on today's technology-enabled battlefield. Yet, while GNSS gives warriors a remarkable advantage, overreliance on the technology has become an exploitable liability in ways that are not even yet fully understood.[86] To overcome this potential handicap, the U.S. Government has wisely "begun to place more emphasis on training warfighters in more traditional skills; reading paper maps, navigating by the stars with the help of sextants, and the use of physical map boards to monitor troop locations on the ground."[87] This is absolutely necessary to counter the

traditional assumption that these technological systems are always accurate and operate without interference. Going forward, it will be important to train tomorrow's warfighter to not only understand the technology, but to understand the assumptions behind the technological output. This will enable the warfighter to ask the right questions, challenge assumptions, and operate seamlessly in both an analog and a technological battlefield.

Chapter 2. Automatic Identification System (AIS)

There are no rogue ships; there are only rogue shipowners. - Barista Uno[88]

The AIS is a situational awareness system whereby vessels and shore stations within a 10–20 nautical mile range can exchange tracking information. With this system, vessels at sea are aware of each other's presence; maritime authorities in littoral states can identify and monitor vessels and cargo in their area of responsibility; and navigation, meteorological, safety, and other items of information can be exchanged between ships and shore stations—including ports. AIS is critically important in the LZ. These waters have the most congestion in terms of the number of vessels; the most hazards to navigation, given the relatively shallow waters of the near coastal zone; and the most danger from IW. A large number of adversaries could operate easily and freely in this part of the ocean.[89] This section provides an overview of AIS, the cyber vulnerabilities of the system, and the implications of these vulnerabilities. Technical details about the operation of AIS can be found in Appendix 3.

SOF and AIS

Most of the technology required to maintain Maritime Domain Awareness is heavily dependent on AIS technology. For many years, U.S. Navy vessels have used AIS in receive-only mode as standard practice to preserve operational security.[90] After a series of ship collisions in the Pacific Ocean, this policy came under review.[91] Commercial vessels operating in international waters typically operate with an active AIS, but often conceal their movements to circumnavigate criminally active waters.[92]

AIS can serve as a warning to those conducting counter-piracy operations. Historically, hijackers of commercial vessels have been unfamiliar with the operation of a ship's AIS. This can serve as a warning to those conducting counter-piracy operations; if a commercial ship is not transmitting its AIS signals, or will not send their AIS beacon upon request, it is often a sign of piracy. However, a new trendline in the industry is revealing that

many tech-savvy pirates and proxies have become intimately familiar with shipboard AIS and are fully capable of spoofing the transmissions.[93]

While military vessels may have secure AIS, military ships are not immune to the hazards of AIS vulnerabilities. A malign actor can target a civilian vessel to force a harmful interaction with a military vessel, particularly if the military vessel is invisible to both AIS—due to not transmitting AIS information—and radar, due to naval stealth technology. Likewise, a small irregular force can employ multiple AIS spoofing scenarios in order to masquerade as a larger force; direct commercial or military traffic into undefended or indefensible waters; or coax movement away from a safe port. In addition, a military vessel can alter its own signal to portray a slightly different location, with the intention of negatively impacting the defenses of adversaries.

AIS Security Vulnerabilities

Although AIS was designed in the 1990s, security was not built in to AIS standards until the current OneNet standard—which was released in 2020—appears in products, projected for 2021.[94] Balduzzi et al.,[95] Goudossis and Katsikas,[96] and Kessler et al.,[97] among others, have discussed security vulnerabilities in AIS that identify a variety of attacks on the system.

Balduzzi et al.[98] have identified myriad attacks on AIS based on four primary protocol weaknesses:

1. **Lack of validity checks.** AIS messages contain no geographic validation information, meaning that it is possible for a bad actor to send an AIS message from one location while purporting to be in another location.

2. **Lack of timing checks.** AIS messages do not natively contain a timestamp, meaning that a bad actor can record valid AIS messages and replay them at a later time.

3. **Lack of authentication.** The AIS protocol provides no mechanism to authenticate the sender, thus anyone with the ability to transmit an AIS packet can impersonate any other AIS device.

4. **Lack of integrity checks.** AIS messages contain no message integrity checks, allowing an adversary to intercept and/or modify transmissions.

Because AIS operates on public maritime radio frequencies, anyone with an AIS receiver can hear all the transmissions. While AIS transceivers were relatively expensive at one time, there are many ways today to build inexpensive systems—on the order of $100—to both receive and transmit AIS messages.[99] AIS users also share the broadcast frequency. While efficient in terms of communications resources, this allows an attacker to usurp the bandwidth to deny other devices the opportunity to transmit, impede the shared time slot synchronization process, or change slot reservation/assignment information. Any of these denial-of-service (DoS) attacks can effectively knock other AIS stations off the air or, indeed, render the entire system useless within a geographically localized area.

AIS Spoofing Case Studies and Implications

AIS employs publicly available message formats, transmits on public maritime radio frequencies, and is designed to assume that all transmissions are legitimate and valid. This allows a bad actor to transmit messages of their own creation, to spoof non-existent *ghost* vessels or aid to navigation (ATON), replay earlier AIS traffic, trigger false SAR or CPA alerts, or send bogus weather or navigation information—possibly causing a vessel to alter its course. Data about an existing vessel can even be altered in real time. An AIS DoS attack can cause a local AIS broadcast area to go dark. These attacks are enabled by software tools, commonly available on the internet, that can generate AIS messages.[100]

AIS employs publicly available message formats, transmits on public maritime radio frequencies, and is designed to assume that all transmissions are legitimate and valid.

Figure 5 is a demonstration of the display of ghost vessels. The figure shows symbols for nine vessels in the Daytona Beach, Florida, area, displayed using *OpenCPN*[101] chartplotter software. Details for each vessel can be found merely by clicking on the target. *Chasity Brooke* is a real vessel, as are six of the other targets shown here. *Sea Fox* and one other target are also real vessels but had been in the area six months earlier; their data are being replayed and interjected into the AIS data stream. A bogus vessel could also be injected into the system. It is impossible to tell from AIS alone which ships are real and which are ghosts.[102]

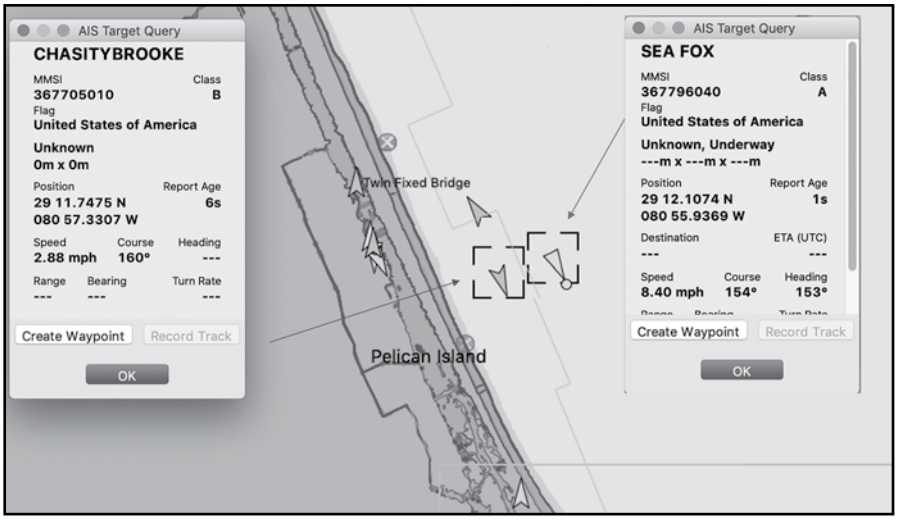


Figure 5. AIS display of real (*Chasity Brooke*) and ghost (*Sea Fox*) vessels off the coast of Daytona Beach, Florida. Source: Gary C. Kessler

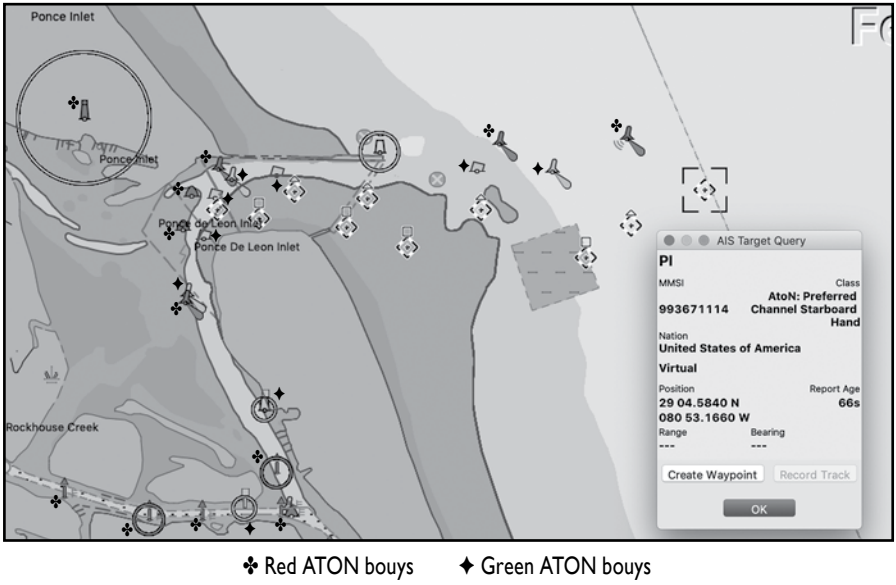


Figure 6. An AIS display of real and fake virtual ATONs is shown in Ponce De Leon Inlet, south of Daytona Beach, Florida. Source: Gary C. Kessler

Figure 6 is a demonstration of ghost ATONs. The figure shows the physical red and green ATON buoys in Ponce de Leon Inlet on the east coast of Florida, marking the portion of the inlet that is dredged to a depth of at least 30 feet (9 meters). The figure also shows a set of virtual ATONs that include a preferred channel marker, labelled "PI," and virtual red/green ATONs defining a second channel on the south side, which is significantly shallower. These virtual ATONs appear on the display based upon spoofed AIS messages. The USCG has sole authority in the U.S. for transmitting information about virtual ATONs, but there is no mechanism with which to authenticate the sender of this information.[103]

Concluding Observations

AIS spoofing is any event where AIS-related displays show bogus information. The earlier discussion of GPS spoofing related to *Stena Impero* off the coast of Iran and the Port of Shanghai were reported as AIS spoofing. The root cause in both cases, however, were spoofed GPS signals, which caused the AIS equipment to display incorrect information rather than spoofed AIS messages. That said, AIS spoofing is also a part of the larger Port of Shanghai story. Smugglers in the area, primarily carrying valuable cargos of banned sand and gravel, have been spoofing AIS signals—pretending to be other vessels—to escape detection by the authorities. The Shanghai MSA reports that illegal sand and gravel vessels accounted for 23 collisions, meaning two moving vessels striking each other—or allisions, meaning a vessel striking a stationary object—on the Yangtze River in 2018 at a cost of 53 lives. The AIS spoofing threat shows no sign of stopping; in June 2019, an oil tanker suspected of smuggling oil had been sending cloned AIS signals and reportedly rammed an MSA patrol boat to evade capture.[104] Reports in 2020 described AIS data showing several boats traveling in circles around the area of Point Reyes, just north of San Francisco, California, although their true positions were confirmed to be in different locations thousands of miles away.[105] Countering AIS jamming and spoofing will be a particular concern for SOF in the future.

Chapter 3. Malware And Maritime Systems

> We worried for decades about WMDs—Weapons of Mass Destruction. Now it is time to worry about a new kind of WMDs—Weapons of Mass Disruption. - John Mariotti[106]

Malicious software—also known as malware—is a threat to all computer systems and the information they contain. This chapter will discuss malware as it applies to the maritime sector. A tutorial providing details on the different types of malware affecting the maritime industry is provided in appendix 4.

SOF and Malware

The SOF maritime systems are far from immune to the effects of malware. Indeed, military cyber targets are of strategic importance in the theater of littoral waters. Cyberattacks today happen at a time when the attacker chooses. Malware attacks are always deliberate, even when they do not target particular victims; advanced persistent threat (APT) attacks are always targeted. Malware can greatly interfere with SOF freedom of maneuver and military communications systems. Yet, with the constant barrage of cyber events, a deliberate attack might be missed in the "fog of war" or the intent of an event misinterpreted, which could cause unanticipated responses.

The ultimate target of a malware-based cyberattack might not be the initial victims—in fact, a common strategy for information operators is to find the weakest link in a supply chain and use that victim as the starting point for an attack targeting a partner. Such attacks might result in supplies not being where they are needed, parts being replaced by counterfeit or otherwise inadequate substitutes, or leakage of mission plans. The use of malware is growing, especially in terms of the sophistication of the applications. From the SOF context, irregular and malicious adversaries are routinely aided by nation-states for whom they are merely proxies. The trendline is growing, and these irregular forces have the capability to conduct "morally ambiguous operations while maintaining plausible deniability."[107]

Malware and Maritime Systems Case Studies

An example of the impact of a cyberattack on a maritime operation is that of the EternalBlue exploit tool NotPetya worm and the Danish shipping company, A.P. Møller-Maersk. The story starts in April 2017 when the hacking group, The Shadow Brokers, provided a large number of cyber exploit tools allegedly created by the National Security Agency (NSA) and Central Intelligence Agency (CIA) to WikiLeaks.[108] One of those tools was called EternalBlue, an exploit for a vulnerability in the Microsoft Windows operating system's Server Message Block (SMB) service.[109] Although Microsoft had released a patch during the previous month, it had not been universally applied by the user community.[110] Furthermore, no patch had been released for discontinued versions of the operating system, including Windows XP, which had an end-of-life in April 2014.[111]

The first EternalBlue-based cyberattack started on 12 May 2017, when the WannaCry ransomware worm started circulating around the world. In the first 24 hours, WannaCry infected tens of thousands of computers in 99 countries throughout the Americas, Asia, and Europe; by the end of the second day, more than 200,000 computers in 150 countries were infected. WannaCry is not known to have specifically targeted any of its victims. It was a worm that traveled around the internet infecting susceptible systems, which included approximately 80 percent of the computers in the UK's National Health System that were still using Windows XP.[112] WannaCry died down a few days later after Microsoft released an emergency patch for older operating systems, and a cybersecurity researcher found a "kill switch" that halted further propagation.[113]

This was not the end of EternalBlue, however. On 27 June 2017, malicious actors released a new worm called NotPetya, which also employed the EternalBlue exploit. Even though Microsoft's patch in response to WannaCry would have also prevented damage from NotPetya, there were still hundreds of thousands of unpatched systems around the world. Unlike WannaCry, which was possibly intended to be a money maker for the attackers, NotPetya appears to have been designed to cause destruction of files and computer systems. Although sites in the Ukraine were the primary targets, any unpatched Windows system could be victimized.

One such victim of NotPetya was Maersk, whose information technology (IT) systems were shutdown network-wide, including their terminal in

the Port of Los Angeles. All of Maersk's network domain controllers were compromised, except one in Ghana that just happened to be offline at the time of the attack due to a power failure. Using that one server, Maersk was able to rebuild its IT communications after replacing their entire network infrastructure of more than 45,000 computers and 4,000 servers. Maersk's network was down for 10 days and experienced a revenue loss estimated around $300 million.[114]

From the maritime perspective, this example is not just about Maersk's network being down and/or disrupted for nearly two weeks, but the ripple effect. The company is responsible for 76 ports around the world and operates 800 vessels that carry tens of millions of tons of cargo every year. Maersk's computer systems manage a complex operational network where a ship enters a port every 15 minutes somewhere around the world, representing nearly 20 percent of the world's cargo shipping capacity.[115]

Ransomware and other forms of malware targeting the maritime industry were particularly prevalent by 2018. In July 2018, for example, there was a ransomware attack affecting the China Ocean Shipping Company (COSCO), the third largest shipping company in the world with more than 1,100 ships and more than 1.5 million cargo containers. The attack focused on Windows systems and impacted the company's internal network and e-mail systems, forcing the shutdown of its terminal at the Port of Long Beach. Within a day, there was widespread network failure across COSCO Americas, affecting e-mail, local websites, and telephone systems in Argentina, Brazil, Canada, Chile, Panama, Peru, the U.S., and Uruguay. As a precautionary measure, COSCO suspended bookings of hazardous and awkward cargo. Although vessels themselves were reportedly not affected, port operations in the Western Hemisphere were disrupted for days.[116]

Ransomware and other forms of malware targeting the maritime industry were particularly prevalent by 2018.

In September 2019, the ports of Barcelona and San Diego reported ransomware infections within five days of each other. Both incidents were caused by ransomware called Ryuk.[117] Ryuk has continued to make the rounds of maritime ports, resulting in a USCG Marine Safety Information Bulletin after the ransomware was found at another U.S. port. In all cases, port operations were disrupted although ships were presumably unaffected.[118] The Australian shipping company, Toll, was hit by two ransomware infections in the

first half of 2020, affecting many of their regional operations; they have a presence at more than 1,200 locations in 50 countries.[119] The infection vector in these cases appears to have been phishing e-mails, clearly indicating that these were targeted attacks. Like many sectors in cyberspace, the maritime industry was literally hammered with ransomware attacks in 2020, with more than a half dozen highly publicized incidents.

In another example, a 2018 malware incident caused the malfunction of a ship's electronic chart display and information system (ECDIS). The ship was designed for paperless navigation and did not carry paper charts, so the departure of the ship from its port was delayed by several days. The crew mistook the failure of the ECDIS as a technical failure, and it was not until a technician arrived from the ECDIS manufacturer that they discovered that both ECDIS networks were infected with a virus. In a second example, a ship's main application server was infected with ransomware that encrypted critical files, which caused complete disruption of the vessel's IT infrastructure and rendered the applications needed for ship operations to be unusable. The incident kept reoccurring even after complete restoration of the server. The root cause of the infection was found to be poor password policies that allowed the attackers to successfully brute force remote management services.[120]

Supply Chain Vulnerabilities

Today's supply chain—both military and civilian—has myriad vulnerabilities due to an incredibly complex, globally interconnected ecosystem that has multiple layers of outsourcing. While using commercial off-the-shelf (COTS) products have lowered costs, decreased delivery times, improved the ability to build innovative solutions, and improved device and system interoperability, it has also added the risk that the buyer ultimately may not know the true source of every component in a system. Risks to the supply chain include the use of counterfeit components, use of unauthorized hardware manufacturers and software developers, theft, alteration, and poor manufacturing or development processes.[121]

The supply chain is a target of malicious access because suppliers often have bona fide credentials allowing them to directly connect to systems behind firewalls and other cyber protections. If a malign actor wants to access a particular target organization and cannot get through the target's

cyber defenses, a common approach is to compromise a supply chain partner's network—which often is not as well defended—and use their access to penetrate the intended victim's system. This can be particularly insidious if the supply chain partner is purposely working with a foreign government.[122]

Another way to gain access, particularly in today's global manufacturing economy, is the installation of malicious software or firmware in hardware shipped by a nefarious or compromised vendor. The U.S. military's dependence on the vast DIB has created avenues for proxies to interfere with the integrity of the supply chain. In one example, a 2014 report revealed that a Chinese manufacturer had installed the Zombie Zero malware in Windows XP-embedded scanners. One victim was a company that tracked packages being onloaded and offloaded from ships, as well as trucks and planes. The data—which included origin, destination, contents, and system data—was then transmitted to the company's central database. Although the company had excellent perimeter security, the scanners were behind the firewall and part of the internal network. The malware was able to compromise the central server—providing the malign actor a foothold within the shipper's network and a pathway to exfiltrate any databases.[123] While this manufacturer has reportedly been removed from U.S. military and government approved vendor lists, the potential issue remains with any untrusted manufacturer and/or port authority.[124]

Another way to gain access, particularly in today's global manufacturing economy, is the installation of malicious software or firmware in hardware shipped by a nefarious or compromised vendor.

Chinese manufacturers also have a history of building keystroke loggers into hardware and software keyboard products they produce.[125] Yet, products from Chinese manufacturers are not the only susceptibility. In some cases, Chinese products are re-packaged and fraudulently labeled as "Made in the U.S.A." by American companies, which adds to the complexity and serpentine character of the supply chain issues.[126]

Concluding Observations

Maritime cyber events are not isolated incidents; on the contrary, they are on the rise. Shipboard, port, and other maritime networks are as susceptible to viruses and other malware as any other computer network. By 2018, several

reports highlighted the growth in cybersecurity issues aboard ships and in ports, where researchers have found numerous incidents of ransomware, USB malware, and worms.

The implications of the growing trendline in this area are profound for SOF, as all maritime systems need to be protected against malware and other cyberattacks, and no network stands in isolation. The SOF community operates at the tactical end of the conflict spectrum, yet every agency and organization has some communication with suppliers and partners. Maritime and military networks need to address near-continuous threats to the global supply chain. There is an increasing number of threats to maritime and DOD operations where cyber is an instrument, vector, and/or target of the activity. Meanwhile, the supply chain encompasses management of personnel and materiel, as well as communication with ports, allies, civilian vessels, and suppliers.[127]

Looking to the future, the SOF community will be challenged with ensuring the safety of its personnel, while simultaneously creating a meticulous and rigorous method for protecting military networks, and the materials and goods from the global supply chain. Across the government, several agencies have identified best practices in managing the risk from foreign entities and malign actors, many of which can be adapted for the SOF enterprise. These best practices include, but are not limited to:

- developing rigid guidelines for acquisition professionals, and ensuring contractors adhere to industry standards;
- identifying Supply Chain Risk Managers to act as stakeholders for standards;
- ensuring contract language includes an audit capability for the supply chain;
- educating and training professionals in the organization about the risks inherent in the supply chain; and
- encouraging continual assessments, exercises, and auditing of the entire process.

Chapter 4. Cyber-Physical Systems (CPS)

> It's expected that the cyber-physical systems revolution will be more transformative than the IT revolution of the past four decades.
> - Hausi A. Müller[128]

CPS is a broad term, referring to the integration of the cyber and physical worlds by combining computers, machinery, and people to form operational systems. CPS is a disruptive technology, combining computation, communications, and control as an enabler for smart infrastructures and industrial applications in all aspects of human life and across all critical infrastructure sectors. Nowhere is this truer than in transportation and, particularly, in the maritime transportation sector. This chapter will introduce CPS and related terminology, its impact on the MTS—particularly important in the LZ—and some of the cybersecurity aspects affecting maritime use of CPS technologies.[129] CPS technologies are described in detail in appendix 5.

The pinnacle of CPS is the IoT, the concept of combining various enabling technologies in new ways to provide new services. IoT combines data analytics, advanced sensors, and new software to allow individual devices to share information and participate in system-level decisions, transforming conventional physical devices into smart ones. The enabling technologies and functions used in IoT systems are not new. What is new is the ways in which they are connected and work together, the ability to enable innovation, and the seemingly endless machine-to-machine and people-to-machine applications.[130]

The significance of IoT cannot be overestimated. Consider that there were 15.4 billion IoT devices worldwide in 2015. That number doubled to 30.7 billion by 2020, and it is estimated to more than double again to 75.4 billion by 2025—which represents more than nine IoT devices per person.[131] Applications are found throughout critical infrastructures and other aspects of human endeavor—including smart cities, connected healthcare, smart agriculture, connected industry smart supply chains, smart power, and smart retail. The transportation sector has many IoT applications, including the connected car, smart airports, and, of course, smart ships and ports.[132]

SOF and CPS

Within the United States, the USCG has responsibility for the maritime transportation system, including ports, vessels within U.S. waters, inland waterways, and U.S. near coastal waters.[133] As the U.S. military defines a strategy to protect MTS CPS technologies, malign actors are actively seeking to stockpile zero-day exploits—vulnerabilities that have not been patched or made public—as offensive cyberweapons. From the SOF perspective, the security risks posed by the proliferation of networked devices leaves tacticians exceedingly vulnerable. It is difficult for the military to perform operations without being detected, and even harder to conceal day-to-day operations. The sheer proliferation of networked devices—much of those including COTS equipment—provides malign actors penetration points for data mining, surveillance, and other nefarious activity.

As the U.S. military defines a strategy to protect MTS CPS technologies, malign actors are actively seeking to stockpile zero-day exploits—vulnerabilities that have not been patched or made public—as offensive cyberweapons.

CPS Applications and Cyber Implications in the Maritime Sector

Modern merchant and military vessels are increasingly complex and have been introducing new forms of automation for decades. Shipboard automation has, by and large, augmented human operators and engineers, and made operations safer and more efficient.[134] Individual automated systems on ships have evolved into an integrated ship model where systems are increasingly intertwined.

Many shipboard functions are controlled automatically so that systems can maintain their states according to preset parameters—such as the temperature of cooling water, fuel viscosity into the engine, speed and course over ground, or ballast tank levels. This automation allows a vessel to get by with fewer crew members, and also provides some functions that would be almost impossible to carry out manually with the same level of precision. As an example, a ship's dynamic positioning system can maintain a nearly exact position by using a set of thrusters to accommodate for surge, sway, yaw, wind, current, waves, and other forces; manual control of such a system would be practically impossible.[135]

Shipboard automation has, historically, improved the ability to manage, monitor, and control existing shipboard subsystems, such as:[136]

- hull, mechanical, and electrical systems
- warfare systems
- shipboard electricity
- propulsion and maneuvering systems
- auxiliary machinery
- traditional and nuclear power plants
- ballast systems
- navigation
- cargo systems
- emissions
- surveillance systems

New and innovative systems are made possible by emerging CPS and IoT technologies. Some examples of new ways to use computers and communications in maritime include:

Digital rope. Using embedded sensors, mooring lines can monitor tension, time, and temperature, and can provide early detection of wear and failure; the lines can communicate back to an app on the bridge.[137]

Equipment maintenance. Traditional Interactive Electronic Technical Manual maintenance systems can be augmented with CPS technology to automatically and proactively collect and analyze data; rapidly improving the speed and accuracy in detecting and repairing faulty equipment.[138]

Intelligent container terminals. Approximately 90 percent of the world's cargo is transported by ship, and these cargo vessels themselves are getting larger and larger. Maritime container traffic has become a fast-growing segment in the shipping industry, and ports have become the bottleneck in the movement of cargo. Optimization of the process requires communication between all elements in the near coastal supply chain— namely, the vessels, ports, maritime terminal, and cargo handling systems. CPS/IoT technologies have been key to the creation of a cooperative cognitive maritime cyber-physical system to provide high-speed, low-cost communication between ships, ports, buoys, oil/gas platforms, and shore stations, including the full or partial automation of cranes and transport vehicles at the ports.[139]

As suggested by this short list, IoT concepts can be applied to any maritime system, limited only by our imagination and creativity. The concept of shipboard IoT, or Internet of Ships, merely recognizes that current and emerging information and communications technology (ICT) systems, appropriately provisioned and configured, can allow system designers to better leverage existing mechanical and technical assets, enable innovation, build scalable systems, improve efficiency and agility, and make a big impact on operations with small changes. New ways of using sensors and CPS enable many types of integrated shipboard systems, from the bridge to the engine room.[140] As a master knows more about the state of the ship, this information can also optimize supply chain operations, ensuring that fuel and other supplies are precisely where they need to be precisely when they need to be there.[141]

Maritime CPS equipment has the same potential security vulnerabilities and weaknesses as other computers. As an example, the Auto-Maskin DCU 210E engine supervision unit, RP 210E remote touchscreen panel, and Marine Pro Observer app are a set of hardware devices and smartphone apps used to monitor and control ship engines.[142] In 2018, they were found to have several authentication and encryption vulnerabilities—including the use of an undocumented remote access server using hard-coded username and password; an undocumented protocol with which to communicate with other devices without any validation procedure; cleartext transmission of sensitive information; and an embedded web server that transmits the administrator personal identification number in plain text. These flaws could allow an attacker to access and control any connected engines, determine what sensors are present and in use on the ship's network, determine system configurations and settings, and send arbitrary control messages to the engine control units.[143]

Maritime CPS equipment has the same potential security vulnerabilities and weaknesses as other computers.

IoT camera systems have also been targeted by bad actors. In 2017, a Louisiana-based maritime company reported that cameras on a quarter of its small fleet of boats had been compromised. In this case, Dahua DHI-HCVR systems were accessed remotely via the Web by exploiting a weakness in the camera's authentication procedures; the camera's contrast settings were set to darken the resolution, effectively blinding the camera.[144] Other reports

emerged that this same camera had previous issues where remote users could circumvent authentication and 13 other vulnerabilities that dated back as far as 2013.[145] In 2018, camera images from Moroccan-flagged fishing vessel *Mist* were posted to Twitter and claimed to have been taken remotely over the internet. The reports could not be confirmed because of missing metadata,[146] but the images appeared legitimate and certainly plausible.[147]

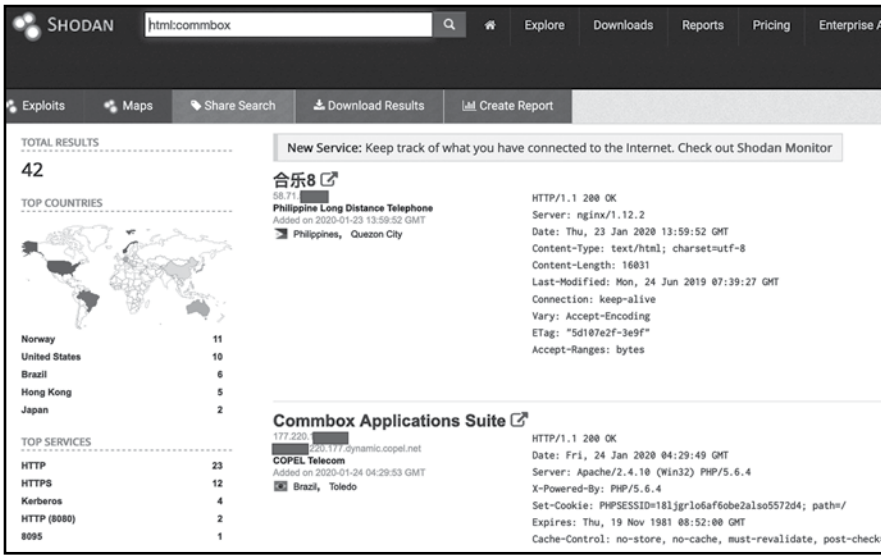


Figure 7. Shodan is used to find vulnerable IoT systems. Source: Shodan/used with permission

Communications systems are particularly vulnerable targets because, by definition, they have a connection to outside, public networks. With IoT devices, however, the problem is exacerbated by internet tools that aid in finding vulnerable communications systems (figure 7). One of the first widely reported attacks on a communication antenna targeted the Cobham Sailor 900 very small aperture terminal system,[148] which had a buffer overflow vulnerability allowing an attacker to bypass login authentication and execute remote code.[149] This problem is not unique to one product or one manufacturer, and many reports subsequently emerged about vulnerable communications terminals, buffer overflows, and weak password management (e.g., a null username or a username of *bridge* with a password of *12345*).[150]

Accessing a communications terminal via IoT databases has also been reported as a vector to do significantly more damage, including turning the

devices against people. Presentations at Black Hat 2014 and Black Hat 2018 demonstrated vulnerabilities in satellite communications (SATCOM) terminals that included software backdoors, insecure communications protocols, and buffer overflows. If exploited, these vulnerabilities could:[151]

- disrupt, intercept, or modify onboard SATCOM
- attack crew's devices
- control SATCOM antenna positioning and transmissions
- perform high intensity radiated field cyber-physical attacks
- reverse engineer product backdoors in order to gain access

As noted earlier, automated ship systems have been in use for many decades. The vulnerability of software-controlled systems became evident in the early days of automated ballast systems. *Ms Zenobia* was on her maiden voyage from Sweden in June 1980. During the first leg of the trip, *Zenobia* started listing to port due to excess water in the ballast tanks; after being righted, she continued on her journey. At Larnaca, Cyprus, her list reoccurred due to a software error in the computerized pumping system and she was towed out of the harbor as a precautionary measure. The automatic system continued to pump water, and when *Zenobia* reached a 45 degree list to the port, the Larnaca port captain refused her re-entry. *Zenobia* capsized in 138 feet (42 meters) of water, with no loss of life.[152] Although not a cyber-attack—in that there was no external manipulation of the software—this is an object lesson that automated software systems are a vector for harm. Software can be manipulated through the use of malware or bogus updates, and manual overrides can save ships, cargo, and lives.

Two additional examples help to illustrate the fragility of vessel stability and how software vulnerabilities can be a potential vector for harm to ships. In 2015, high-end car carrier *Hoegh Osaka* ran aground after leaving Southampton and was stranded in The Solent—the strait separating the Isle of Wight from the English mainland—for 19 days. Due to the vessel being unstable before leaving port, *Hoegh Osaka* developed a 40 degree starboard list, leaving the rudder and propeller out of the water. Shifting cargo resulted in a hull breach, allowing seawater to enter. In this case, the ship was near a deep-water channel and sinking would have blocked container ships, passenger ships, and ferries. The investigator's report indicated that there was a significant difference between the actual and estimated cargo weight, resulting in unsafe stability calculations.[153] In 2019, vehicle carrier *Golden Ray* with

a cargo of 4,200 vehicles was grounded in St. Simons Sound, Georgia, United States. The vessel started to list approximately 23 minutes after it left port; the pilot on board deliberately grounded the ship so that she would be out of the channel. She later rolled over on her port side. Even though *Golden Ray* was grounded out of the channel, the Port of Brunswick was closed for four days; if it had capsized in the channel, the effect on the port would have been far longer lasting.[154] The instability of these ships was most likely due to human error, but the load management software certainly demonstrates a lucrative target for cyber attackers.

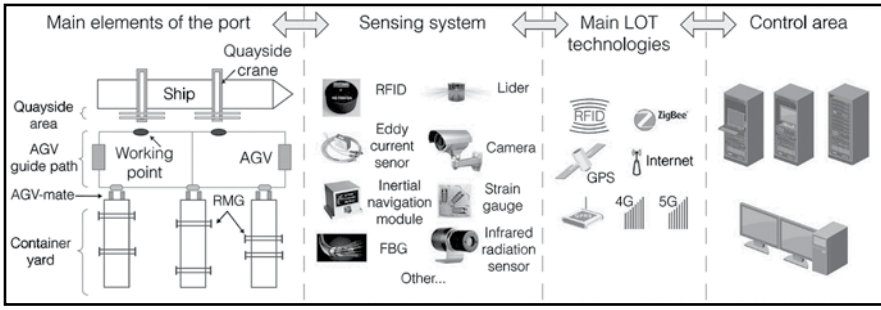


Figure 8. The layout of an automated container terminal. © 2018 IEEE. Reprinted, with permission, from Yang et al., "Internet of Things for Smart Ports: Technologies and Challenges," IEEE Instrumentation and Measurement Magazine 21, no. 1

CPS and IoT transformation of the MTS is not limited to just ships. Today's ports comprise a complex infrastructure of ICT, machinery, business processes and transactions between trading and supply chain partners, regulations, and stakeholders. This includes port owners, port authorities, port operators, unions, shipping and other transportation companies, and, in some cases, the military.[155] Digitalization in the form of combining IoT, CPS, big data, and machine learning (ML) provides an incredible opportunity for ports to optimize their operation. Improving the organization and timing of ship movements in a busy port to optimize transit, berthing, and loading/unloading, for example, can save both ports and shipping companies tens of thousands of dollars for every hour of decreased down time.[156] Using a combination of sensors, gauges, cameras, radio frequency identification, and other IoT devices—coupled with advanced technologies such as GNSS, internet, Wi-Fi, and 4G/5G mobile communications—container terminals can be automated to optimize the interoperation of cargo ships, rail mounted gantry cranes, and automated guided vehicles. See figure 8.[157]

These technologies and ideas are being implemented at ports today. As an example, the Port of Rotterdam—which handles 140,000 ships and 461 million tons of cargo annually—is working with IBM Corp. to build the "world's smartest port" using IoT technology. Sensors measuring water temperature, water depth, speed and direction of current, tide, speed and direction of wind, berth availability, and other factors at the 41 square mile (106 square kilometer) port will feed centralized information to a dashboard app on connected vessels. This data will streamline port operations to reduce wait times; optimize dock, load, and unload times; and maximize the throughput of vessels at cargo terminals.[158] Similar intelligent ship management, intelligent traffic flow, and smart port logistics systems are being built at the Port of Le Havre.[159]

These initiatives are massive implementations of hardware, software, and communications, including the development of new apps. But, like all IoT components, the potential for attacks on CPS hardware and software is ever present. Suppose, for example, a bad actor hacks or otherwise manipulates a sensor subsystem to send bogus AIS or smart port app messages; or an attacker spoofs AIS clearance time to enter port, marine traffic signal, berthing data, or tidal window messages causing a disruption in vessel traffic. The resulting confusion could disrupt port operations potentially for long periods of time.

Concluding Observations

While many technologies—including CPS and the internet itself—can be an equalizing factor between a large and small organization, agency, or military force, too much dependence upon technology can also be an Achilles' heel. IoT devices on maritime vessels and at ports can allow a single person to do the work of several, thus becoming a force multiplier, but overdependence on technology can cause systemic errors, delays, and inefficiencies if that technology fails. Computer-based ICS use processor chips, sensors, and other hardware components that are

While many technologies—including CPS and the internet itself—can be an equalizing factor between a large and small organization, agency, or military force, too much dependence upon technology can also be an Achilles' heel.

manufactured overseas; malware or backdoors could be inserted into software or, Stuxnet-type vulnerabilities could be built into hardware.[160] Because of the huge number of IoT devices and the relative security weaknesses of those devices, CPS is an attractive target for cyberterrorists and adversarial cyberwarriors.[161]

While CPS and IoT have unique cybersecurity challenges, defense of the computers at the heart of these systems starts with following best practices for securing networked systems such as a defense-in-depth strategy that includes anti-malware, firewalls, intrusion detection/prevention systems, and user training. Using *red teams* to perform external network reconnaissance, vulnerability scanning, and penetration testing can also yield a tremendous amount of information to help better secure a network.[162] Another emerging strategy in the defense of CPS is the use of digital twins, a virtual representation of a physical object or process. The U.S. military is already using digital twins to secure semiconductors and to test GPS.[163] Combining IoT software systems with the real time digital twin of managed hardware provides a better understanding of the entire CPS system—including the weaknesses, vulnerabilities, and potential exploits. With this knowledge, operators can better adjust the efficacy and security of their systems.[164] One such maritime initiative is the ProProS research project at the Fr. Lürssen shipyard in Bremen, Germany, which is building a digital twin to control and optimize their manufacturing and assembly processes.[165] Looking ahead, this model for the future—robust systems for counter intrusion as well as digital twins—is likely the most prudent, adaptable, and inherently sophisticated path forward.

Chapter 5. Autonomous Vessels

> The [vessel] of the future will have only two [crewmembers], a man and a dog. The man will be there to feed the dog. The dog will be there to keep the man from touching the equipment. - adapted from Warren Bennis[166]

Autonomous maritime vessels, also called maritime autonomous surface ships (MASS), represent a natural convergence of thousands of years of evolving ship and harbor technology with decades of evolving computing and communications technology. Conceptually, autonomy seems like a good fit in the maritime transportation system, particularly in the LZ where there is an abundance of vessel traffic and natural hazards that automation can help manage and control. But, as discussed earlier in this report, computer-based systems, most notably operational technology (OT), ICS, and IoT, are susceptible to many types of cyberattack. This chapter will review some of the drivers for autonomous vessels and their cyber vulnerabilities.[167] Appendix 6 contains a background introduction to the topic.

Autonomous military vessels have been a specialized area of research in the general field of autonomous ships. Autonomy for military vessels brings many of the same advantages as in commercial shipping but, of course, also adds the fact that autonomy can be a force multiplier and remove humans from places of harm. The U.S. Navy has had a program for developing an unmanned surface vessel (USV) fleet since 2012. Several prototype vessels have been built or are under development, and have already been tested operationally as part of a carrier strike force, and a fleet of seven is expected by 2023.[168] The Navy has already identified many potential uses for autonomous vessels, including roles in missile attack forces; mine search, detection, neutralization, and delivery; antisubmarine and surface warfare; support of SOF; maritime interdiction and security; and EW.[169] While most of the USVs are unarmed, the Navy is also testing armed, unmanned patrol boats for port security, such as a 40 foot (12 meter) remote-operated USV—armed with a .50 caliber machine gun station—to protect warships at anchor.[170] As with a manned vessel, operation of a USV will be more difficult in the LZ than in more open water.

SOF and Autonomous Vessels

Militaries, policymakers, and malign actors around the globe recognize the competitive advantage of autonomous vessels. Much like their airborne counterparts, autonomous vessels are cheaper, operate with less human risk, and can operate for lengths of time well beyond human capacity. An autonomous vessel allows SOF to act from a distance in common operations such as hostage rescue and antipiracy. Unmanned vessels can transmit sensory data to a remote command post, and some can get close enough to hostile maritime vessels to override their controls. Yet, because of their sophistication, autonomous vessels are especially vulnerable to increasingly complex and destructive actions, which poses a unique threat to SOF.

Cyber Threats to Autonomous Vessels

Artificial intelligence (AI), IoT, and mobility systems have been major disrupters in the maritime industry. Autonomous systems in the MTS are at the intersection of innovative uses of advanced technology and vulnerability to all imaginable cyberattack vectors. Cyber technology is the enabler of incredible potential advances but also provides potentially existential threat and attack vectors.[171] The current environment might be summarized as "automation, integration, and remote monitoring meet the internet":[172]

- **Automation.** Maritime machinery and systems are increasingly controlled by software
- **Integration.** Multiple shipboard systems are increasingly interconnected
- **Remote Monitoring/Control.** Land-based offices use ship-to-shore communication to continuously monitor and/or control shipboard equipment
- all these systems are connected to the internet with its 4.5 billion users

Each individual segment above has its own cyber vulnerabilities. As an interconnected system, the potential vulnerabilities and cyberattack vectors are so complex as to be impossible to be fully understood, regardless of whether this is applied to manned or unmanned maritime vessels. The defense requires good software discipline, policies, and controls that limit how one system interacts with other systems, as well as implementing the best cybersecurity design principles, including:[173]

- **Isolation.** Run tasks so that they cannot communicate with other tasks unless there is a trusted relationship.
- **Modularity.** A task only needs to know how to interface with another task but not the internal structure of that other task.
- **Minimization of implementation/least common mechanism.** Avoid sharing parts of security mechanisms among different users, processes, and/or parts of the system.
- **Complete mediation.** All accesses to objects should be checked to ensure they are allowed every time access is attempted (i.e., do not cache access permissions).
- **Least privilege.** Processes should be assigned the least level of privilege necessary to perform their task.
- **Reluctance to trust/minimize trust surface.** Assume that the environment in which the system resides is insecure.

To implement any security defense mechanism or protection, a risk assessment must be performed to identify the actual threats, vulnerabilities, and exposures, as well as to prioritize those risks.[174] Cyber risks for autonomous vessels are due to the addition and reliance on ICT, but as all autonomous vessels do not have the same level of autonomy, the risk factors will vary based upon the vessel's exposure in cyberspace. Tam and Jones[175] propose a risk assessment model for assessing autonomous vessels—shown in table 2—by defining three axes: level of vessel autonomy, value of the exploit to the attacker, and ease with which an attack can occur.[176]

1. On the ship autonomy axis, the highest tier represents the most complex target, a fully autonomous vessel, and the vulnerability is a function of attack vector, target vulnerability, and effect on the target (e.g., AIS jamming could result in a collision).

2. The attacker reward is a function of attacker type and goal combined with target type and effect (e.g., a cybercriminal launching a ransomware attack could put a company out of business or garner a huge payoff).

3. Ease of exploit is a function of attacker type and available resources combined with the target type and resources (e.g., a skilled hacking organization with standard tools could easily exploit a small vessel's network that does not have adequate cyber defenses). Since this axis measures ease of an attack rather than difficulty, the highest tier represents the simplest attack.

Table 2. Tiers of ship autonomy, attacker reward, and ease of exploit. Source: Tam and Jones/Cyber-Risk Assessment for Autonomous Ships

Tier	Ship Autonomy	Attacker Reward	Ease of Exploit
1	Minimal crew required	Little to no value for attacker; minimal impact	APT, requires capabilities of a nation-state
2	Partial autonomation; local crew for simple tasks	Small value to attacker	Advanced skills, requiring considerable resources (organization)
3	Conditional autonomy, potential intervention by local crew	Average to moderate value to attacker	Moderate skills, requiring significant resources (professional)
4	High autonomy, mostly self-running	Valuable to attacker and third parties	Minimal skills or resources required (basic)
5	Complete autonomy	Extremely valuable to all players; large-scale or significant impact	Little to no skills needed (e.g., script kiddies)

The risk matrix can be further refined by identifying specific areas of vulnerability.[177] Earlier chapters in this monograph have already described some of the attack surfaces in the MTS, but specific areas within autonomous systems include:[178]

- positioning systems
- sensors
- firmware patches/upgrades
- voyage data recorders
- intra-vessel network
- vessel-to-land communication
- remote operation systems
- docking systems

While autonomous systems have their own unique issues, the possible attacks on MASS are like those described earlier for the MTS as a whole—such as code injection; tampering and modifying sensors; GNSS spoofing; AIS spoofing; signal jamming; and communication link eavesdropping and disruption.[179]

Concluding Observations

Cybersecurity planning across SOF should follow the "Vulnerabilities Trumps Threats Maxim," which suggests that it is important to focus on understanding and addressing the vulnerabilities in a system rather than on the perceived threats.[180] Organizing a defense around vulnerabilities means to plan based upon things that can be identified, mitigated, and, possibly, eliminated. Organizing the defense around threats is a poor approach, because the threat landscape is constantly changing. Further, if defense is designed around threats that are incorrect, the defense may be inadequate against an unanticipated threat actor. Focus on vulnerabilities; even if the threats are incorrect, a strong defense will be built.

One of the most promising strategies to mitigate the complex vulnerabilities of autonomous vessels is construction of a digital twin, described earlier in this monograph. Autonomous vessels, including ports and mooring systems, are enabled by advanced digital technology. Building digital twins of these systems is of paramount importance to understanding system complexity and appreciating the new cyber vectors for attacking these systems.[181]

Chapter 6. Implications For SOF

> No battle plan ever survives contact with the enemy. - Helmuth von Moltke the Elder[182]
>
> Mann traoch, Gott läuch (man plans, God laughs) - Yiddish proverb[183]
>
> There's a war out there, old friend. A world war. And it's not about who's got the most bullets. It's about who controls the information. What we see and hear how we work, what we think ... it's all about the information! - Sneakers[184]

Historically, cyber defense has been viewed as trying to keep up with an ever-changing environment of cyber threats and vulnerabilities; a cycle of "find vulnerabilities, fix them, repeat." This whack-a-mole form of defense all but guarantees that defense will always lag behind methods of attack. The overriding implication drawn from this monograph is that IW in the LZ will require a new way of thinking. This does not mean merely adapting old methods to a new battle terrain but of adopting a new philosophy in warfare. Consider the futility of the Maginot Line as France, in the 1930s, prepared to defend themselves against the previous war with Germany.[185] The same is true in addressing issues of cybersecurity and cyberwarfare.

Today's cyber defense demands two fundamental changes in philosophy and outlook. First, understand that the assets to protect and defend are not physical but, rather, logical or virtual. Methods designed to protect physical assets are not adequate to protect cyber assets; cyber defenders must protect data that needs to be protected everywhere it resides. This requires new organizational constructs. Second, hierarchical communication structures—be they human or machine-based—give the attacker the edge; if an attack needs to be reported up through a chain-of-command and sent to a vendor before a defense is distributed, attackers have plenty of time to do a lot of damage. Instead, defenders need flat, knowledge-based mechanisms that can be used to share information amongst appropriate parties at the speed of an attack which, in cyberspace, is literally the speed of light. Defenders need to adapt to reclaim the cyber advantage from the attacker.[186]

Just as autonomous vessels are a disruptive technology in the MTS, maritime activities in the LZ are a disruptive force in terms of IW. Leveraging disruptive technologies requires special planning and new outlooks. While traditional risk management processes and procedures are important to apply to these new problems, planners also need to apply non-traditional methods to risk assessment, management, and planning. Rather than focus risk assessment on specific systems or subsystems within a vessel or an operational domain, scenario-based planning provides a larger perspective to identifying and responding to threats, both cyber and non-cyber. Whereas the common cyber risk management approach looks at a static attack on individual parts of a system, scenario-based planning provides a tabletop, exercise-like opportunity to consider the impacts of a natural or man-made attack on a cyber system, a planned response to such an event, and the next steps that might occur due to nature or an intelligent actor. In this way, by wargaming and red teaming a host of scenarios, planners can better prepare a multifaceted cyber defense.[187]

Rather than focus risk assessment on specific systems or subsystems within a vessel or an operational domain, scenario-based planning provides a larger perspective to identifying and responding to threats, both cyber and non-cyber.

One scenario-based planning methodology employed by USCG is Evergreen. This process is not the typical "what happens if someone spoofs our GPS?" type of planning; on the contrary, it is quite untraditional. Evergreen focuses on future planning based upon a vast number of variables—including technology, politics, the economy, the environment, population demographics, and the state of critical infrastructures. Because the future is uncertain, the Evergreen process starts with several plausible futures; participants then discuss actions that might be taken today to advance to, or avoid, the various futures and achieve success down the road. Participants very quickly come to understand the complex interrelationships between global parameters and variables to identify key uncertainties and major trends. While not cybersecurity-specific, Evergreen is a useful process in the cyber domain; it demonstrates the interconnectedness of the variables in the scenario. Ultimately, the process helps participants to better understand the big picture and offers better planning advice to organizational leadership.[188] This unconstrained thinking broadens the perspective of planners so that they might implement

policies and processes that will lead to an advantageous position further down the road; what some call "reverse engineering the future."[189] While planners do need to anticipate all contingencies, it is best to proactively try to create the optimal conditions to avoid undesirable long-term outcomes.

Concluding Thoughts

This monograph has only touched on the many technology drivers of both offensive and defensive actions at the crossroads of maritime operations and cyberspace. Each will have a major impact on the way offensive and defensive operations are conducted in all domains of war and conflict. These technologies will interpret inputs, make decisions, and initiate responses at computer speeds so that humans will not be able to keep up with each individual action. Computers will also be able to track thousands of seemingly unrelated events to anticipate potential adverse actions, and tell a party when and how to launch preemptive cyberattacks or position their cyber assets accordingly; this also applies to kinetic attacks and defenses.[190] The larger lesson of cybersecurity is that defense is not about the systems, it is about the amount, quality, integrity, timeliness, and availability of information.

For an organization like USSOCOM, that sits at the tip of the spear; they must make rapid decisions, planning, organization, recruitment, retention, and resilience the keys towards building a robust, multidomain defense against current and future irregular adversaries. The future is likely to see more data-driven operations and reliance on the globally integrated DIB. Given the growing complexity of the wartime environment and the types of planning required to mitigate and respond to threats, the maritime special operator of the future must have the ability to integrate, synthesize, and comprehend a wide amount of complex information and process several plausible scenarios at once. It will be imperative for commanders and forces in the field to quickly orient towards evolving changes on the battlefield. This reality has major implications for SOF recruitment and retention. The SOF of the future must be able to recruit the most agile-minded warriors, and retain intellectually capable and intuitive fighters. Likewise, cadres of offensive and defensive cyber specialists, whose primary function is not kinetic warfighting, could be integrated within the most tactical of SOF communities. Furthermore, USSOCOM will need to develop internal processes and a framework to mitigate vulnerabilities in the supply chain and

enterprise-level integrated systems. The onus will be upon the command to stay flexible for the fight, integrate innovative practices, appeal to the next generation of warriors, and organize to respond to new challenges.

Appendix 1. The Littoral Zone (LZ) in Context

Oceanographers classify different parts of the ocean in different ways based upon what aspects of the environment they are studying, e.g., topography, biology, or physics. One of the common classification systems is based on depth. The *pelagic zone* essentially covers the water column from the surface to near the bottom of the sea; the very bottom is the *benthic zone*. The pelagic zone can be further subdivided, based upon the penetration of light; the *photic* zone is the top layer where at least some light penetrates—and, in the upper range, photosynthesis can occur. The *aphotic zone* is the dark water. Each of these zones has further subclassifications beyond the scope of this monograph, outlined in table 3.[191]

Table 3. Classification of oceanic zones. Adapted from Webb, *Introduction to Oceanography*.

Zone	Description
Pelagic	Surface to Near Bottom
Photic	Light Penetration
Aphotic	Dark Water
Benthic	Bottom of Sea
Littoral	Near Shore

While the subdivisions within the pelagic zone are largely based upon depth, it is obvious that there is a natural relationship between the height of the water column and distance from shore. The most nearshore region is the LZ (figure 9). The LZ itself is divided into many subareas, but this zone is where the ocean meets the land; it is generally held to extend out to the near edge of the continental shelf, to depths of approximately 200 feet (60 meters).[192]

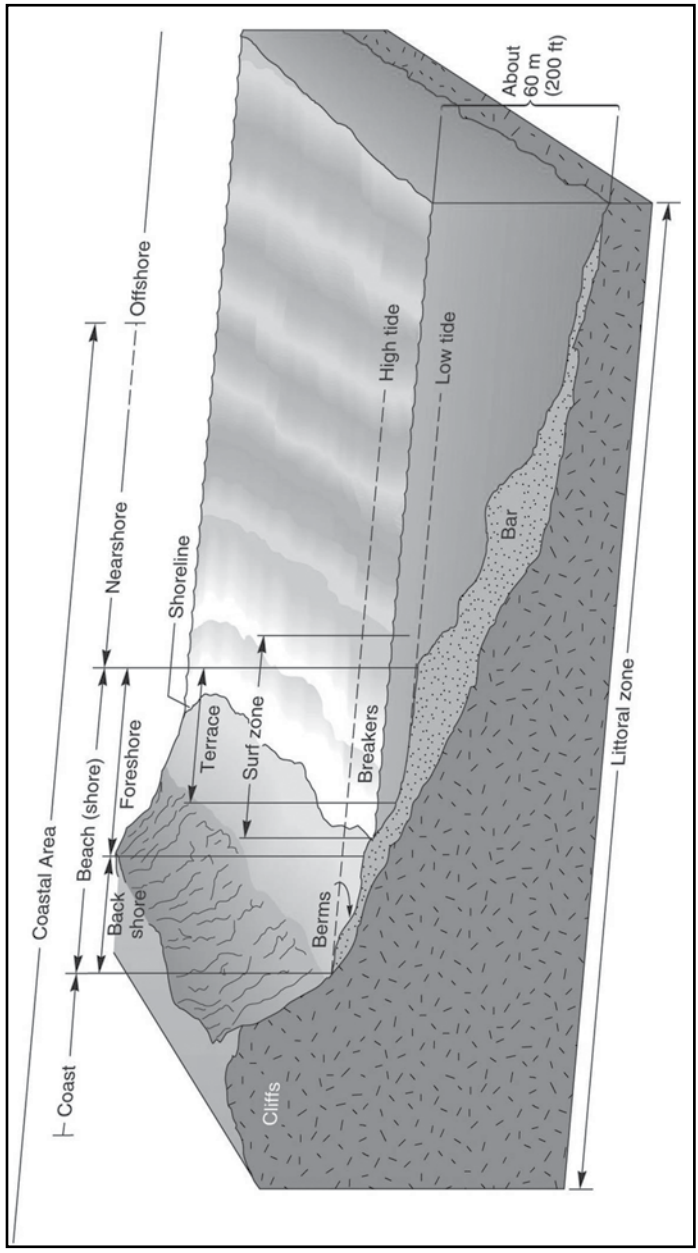


Figure 9. Diagram of the features of the LZ. Source: U.S. Navy

Appendix 2. GNSS and GPS Technical Details

GNSS Overview

Satellite navigation systems employ trilateration as a way in which to determine the latitude, longitude, and altitude of a point on or above the surface of the Earth. Trilateration requires communication with three satellites; it is the relative distance of the receiver to each of these satellites that provides the geolocation capability.[193]

Each GNSS system uses its own constellation of satellites. Each global GNSS constellation employs between 24–35 satellites in a medium Earth orbit (MEO) at an altitude of about 12,000–14,500 miles (19,300–23,300 kilometers). At this altitude, each satellite has an orbital period of 11–14 hours, making one and a half to two orbits a day; they are visible by a given receiver for several hours at a time, as shown in figure 10.[194]

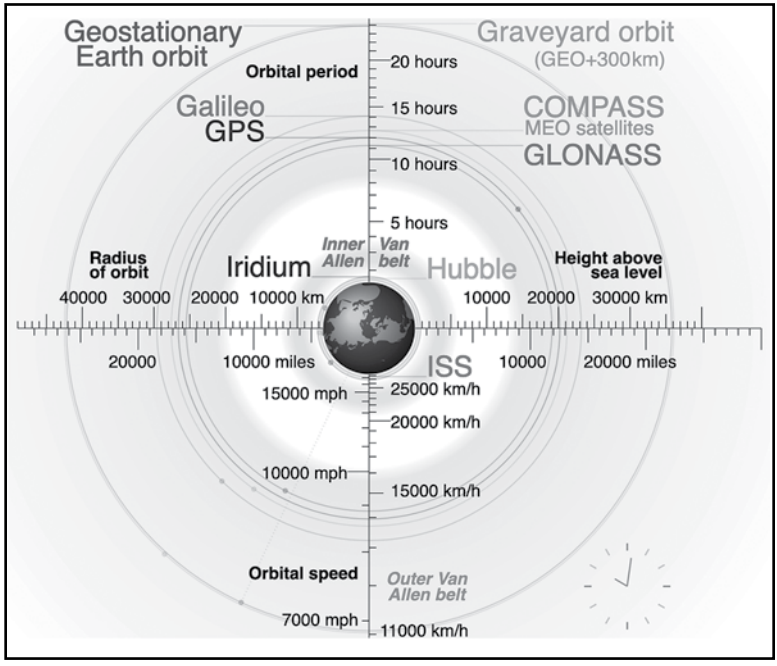


Figure 10. Geostationary, GNSS MEO, and low Earth orbit satellites are compared. Source: Wikimedia

A GNSS receiver can determine its ground position using trilateration from multiple satellite signals; it is, in essence, a passive ranging system. While the satellite transmits a signal at about 50 watts, after traveling thousands of miles the received signal might be as low as 10^{-16} watts.[195] A maritime GNSS receiver overlays its position information on a chart to determine such information as latitude, longitude, altitude, speed, heading, and estimated time of arrival to a destination, as shown in figure 11.

Figure 11. A typical maritime GPS chartplotter display is shown. Source: Garmin/ used with permission

GNSS satellites transmit signals in the UHF L band, which employs radio frequencies in the range of 1–2 GHz.[196] The satellites typically transmit on at least two frequencies simultaneously, commonly called Link 1 (L1) and Link 2 (L2). All satellites in a constellation share the L1 and L2 frequencies, using a multiplexing scheme called code-division multiple access (CDMA), a form of spread spectrum technology also used by mobile phones. Each GNSS satellite is assigned a unique pseudorandom noise (PRN)[197] sequence, which is merely a long string of zeros and ones. The PRN is used to modulate the satellite's transmission on the L band. Receivers know the PRN assigned to each satellite, thus allowing them to synchronize with the signal from a particular satellite. While the CDMA signal is at an extremely low power

level, the code correlation properties of the PRN allow the receiver to recover the signal and the information it contains.[198]

Although geolocation using trilateration only requires three satellites, precise GNSS position and timing requires that the receiver acquire a signal from four satellites. GNSS positioning is based upon a passive reference to a satellite that is moving at a speed of about 2.5 miles a second (4 kilometers a second). Trilateration using three satellites provides an approximate location with an error of up to one mile (1500 meters) due to a lack of synchronization between the satellite's highly accurate cesium clock and the receiver's less accurate clock. A given receiver's clock error—or *bias*—affects all observed satellite signal transit times in the same way; meaning that all of the ranges will be too short or too long by some common ratio. This is known as a pseudorange. By employing a fourth satellite, the pseudorange error can be reduced so that the position estimate is within a few feet (1 meter), effectively transferring the high accuracy of the satellite clock to the surface receiver.[199]

In the vernacular of GNSS, the constellation of satellites is called the space segment and the collection of receivers is referred to as the user segment. The global network of ground facilities that track the satellites, monitor their transmissions, and send commands and data to them is called the control segment.[200]

GPS Technical Background

Currently managed by the U.S. Space Force, GPS—officially, *NAVSTAR, the Global Positioning System*—began as a joint project of the U.S. Air Force and U.S. Navy in the late 1960s, and is generally considered to be the first GNSS.[201] While the military originally intended itself to be the sole user of GPS, the U.S. government's posture since the first satellite launch in 1978 has been that civilians would have access to the system. Civilian GPS products became widely available in the 1990s as the system became fully operational; the signal precision was purposely degraded by the introduction of controlled timing errors, a feature known as Selective Availability (SA). The civilian-oriented service is known as the Standard Positioning Service (SPS); the SA feature was removed by EO in 2000 and is no longer available in current satellites.[202] GPS also provides a Precise Positioning Service (PPS) for the U.S. military and allied nations.[203]

GPS uses a constellation of up to 31 satellites, each of which orbits the Earth twice daily. GPS employs three frequencies in the L band for transmission of navigation messages, denoted L1 (1575.42 megahertz [MHz][204]), L2 (1227.60 MHz), and L5 (1176.45 MHz).[205]

GPS satellites transmit navigation messages on each frequency at an extremely low bit rate (50 bits per second); it takes 12.5 minutes for an entire message to be transmitted and then received by a ground station. Navigation messages include the following information:[206]

- GPS date, time, and week number
- satellite status and health
- ephemeris (position and velocity) data
- clock bias parameters
- almanac (coarse ephemeris data for all GPS satellites, allows receivers to know which satellites are available for tracking)

A GPS satellite is continually transmitting navigation messages. A GPS receiver derives positional information by passively determining the location of, and range to, each of the satellites to which it is listening. Part of this process necessitates the receiver recovering the clock signal from the satellite transmission; the processing power of the receiver has a great deal to do with the accuracy and precision of the reported location. The PRN codes described above are essential to the recovery of the clock, so they are sometimes referred to as ranging codes.[207]

The L1 band is used to transmit navigation messages and uses two PRN codes. The first code, called the coarse/acquisition (C/A) code, was designed to support the SPS and is freely available to the public for civilian use and standard precision applications; this signal is referred to as L1C. The second code is called the precision (P) code and is intended to support military PPS.[208] The P code is encrypted and becomes known as a Y code, but common nomenclature is to refer to this as a P(Y) code. The P(Y) code provides better interference resistance than the C/A code, which makes military GPS more robust and resistant to spoofing than civilian GPS. The military makes the P(Y) code decryption key available to authorized users, including military allies.[209]

Historically, the L2 band was used to transmit the P(Y) code and was intended exclusively for military applications. On newer GPS satellites, the C/A code is also transmitted on L2—referred to as L2C—providing a second

publicly available code for civilian users. Even newer GPS satellites are transmitting a third civilian signal on the L5 band.[210]

The National Marine Electronics Association (NMEA) defines standards for the interface between marine electronics equipment. The NMEA 0183 interface standard message format is character-based and is commonly used on commercial and military vessels.[211] As an example, a message containing GNSS fix data might appear as:

```
$GPGGA,123519,1231.225,N,07002.642,W,1,08,0.9,11.4,M,46.9,M,,*62
```

Among other things, this message indicates that it was sent by a GPS device at 12:35:19 Coordinated Universal Time (UTC),[212] is at a position of 12°31.225'N, 070°02.642'W and an altitude of 11.4 meters (e.g., the receiver is located at the top of the ship's superstructure), has an SPS fix quality, and is tracking eight satellites.[213]

Appendix 3. AIS Technical Details

AIS Overview

The AIS is a tracking system whereby vessels and shore stations within a 10–20 nautical mile range can exchange position, course, and other vessel-related information. With this system, vessels at sea are aware of each other's presence; maritime authorities in littoral states can identify and monitor vessels and cargo in their area of responsibility; and navigation, meteorological, safety, and other items of information can be exchanged between ships and shore stations, including ports. The need for AIS was prompted by the oil spill caused when Exxon Valdez ran aground in Prince William Sound, Alaska in 1989. AIS was designed as a maritime situational awareness system in the 1990s and was adopted internationally in the 2002 International Convention for the Safety of Life at Sea (SOLAS).[214]

SOLAS Chapter V "Safety of Navigation" requires ships of a certain size and/or function to carry AIS transceivers as a necessary safety measure, along with radar, radios, and life jackets. In the U.S., this same mandate is found in the United States Code of Federal Regulations.[215] Ships of 300 or more gross tons traveling internationally, commercial power vessels of 65 or more feet (19.8 or more meters) in length, and power vessels certified to carry more than 150 passengers are among the vessels required to carry AIS Class A devices. Warships are specifically exempted from these requirements, although most modern warships have AIS capability, including the ability to shut it off and/or operate in an encrypted mode.[216] Class B devices can be employed on vessels that use AIS but have no legal requirement to do so, such as large yachts and small fishing boats. AIS devices generally transmit position information messages every 2–180 seconds, depending upon the ship's class, speed, and rate-of-turn. Class A devices generally transmit more detailed information with more power than do Class B devices.[217]

AIS has evolved to be an essential part of a ship's navigation system and is used today primarily for situational awareness and collision avoidance among ships, vessel traffic management, and coastal surveillance.[218] A ship using an AIS receiver can view the local traffic and quickly determine another ship's name, its International Maritime Organization registration number, size (length, beam, and draft), position (latitude and longitude),

course, heading, destination, cargo, status (anchored, moored, underway under power or sail, etc.), and other information as shown figures 12 and 13. AIS gathers its location information from the ship's GNSS so is highly dependent upon the integrity of the navigation system.

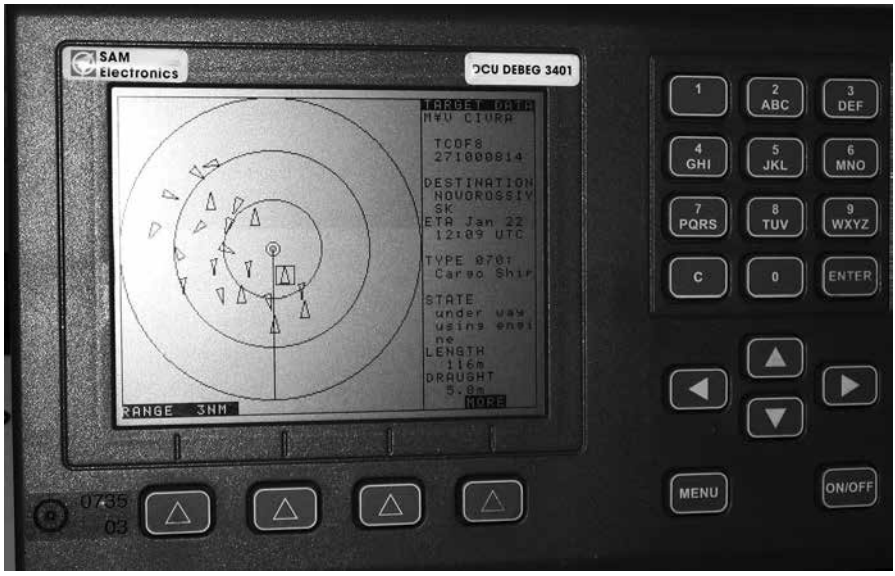


Figure 12. Typical Class A AIS display and control unit with radar-like display of nearby targets is shown. Source: Clipper, Wikimedia Commons CC BY-SA 3.0

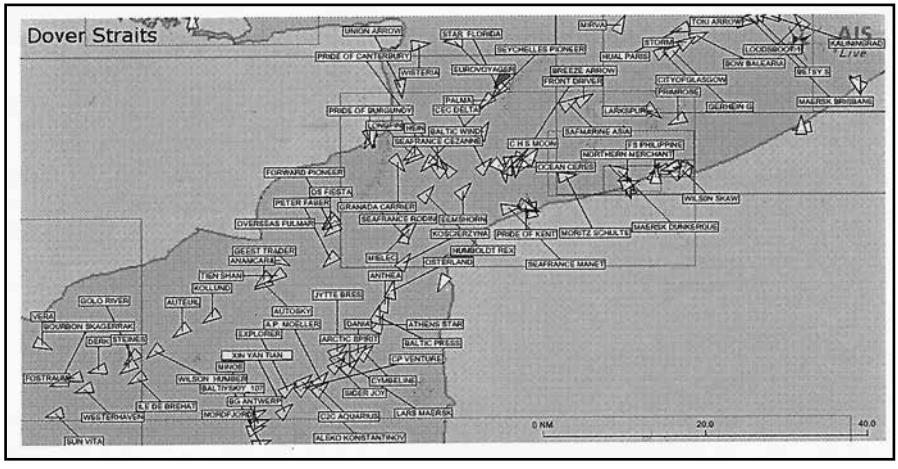


Figure 13. Chartplotter display including AIS data, shows ships in the local area. Source: Wikimedia Commons public domain

There are many active components in the AIS network, shown in figure 14. In addition to ships and boats, other mobile stations include AIS SAR transponders, man overboard transmitters, Emergency Position Indicating Radio Beacons, AIS-equipped satellites, and SAR aircraft. Fixed AIS stations include AIS base stations, repeaters, and specially equipped aids-to-navigation. GNSS satellites are not a direct component of AIS, but they provide essential geographic positioning information to all the mobile components.[219]

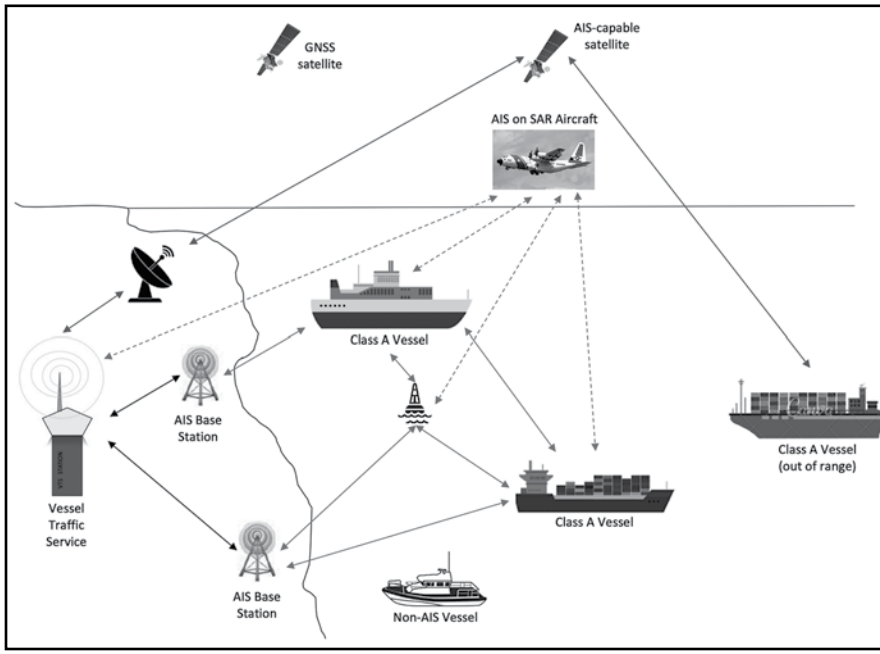


Figure 14. Stations in the AIS network are shown. Source: Gary C. Kessler

AIS Technical Background

AIS is a radio-broadcast communication system, using very high frequency channels 87B (161.975 MHz) and 88B (162.025 MHz) in the maritime band. Radio transmission aspects of AIS, including frequency sharing and time slot reservation schemes, as shown in figure 15, are described in International Telecommunication Union, Radiocommunication Sector (ITU-R) Recommendations M.585-8 and M.1371-5.[220] The primary AIS identifier is the Maritime Mobile Service Identity (MMSI), uniquely assigned to all vessels by international standardization and local maritime authorities.[221]

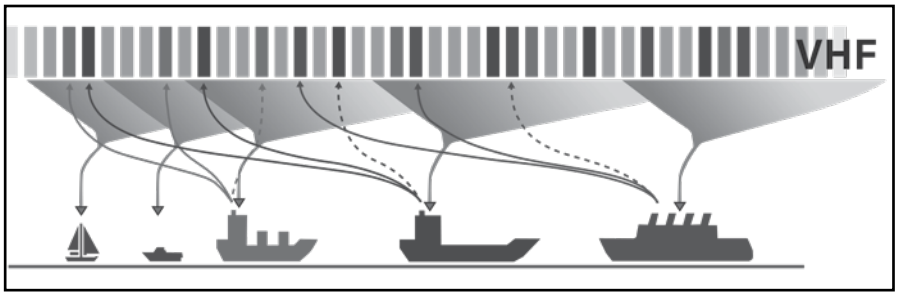


Figure 15. Frequency sharing in the AIS network uses self-organized time division multiple access. Source: AIS Reporter/used with permission

The AIS communication protocols are defined in a family of NMEA standards:

- NMEA 0183 defines character-based message formats at speeds up to 38,400 bits per second over a serial connection[222]
- NMEA 2000® describes binary message formats at speeds up to 250,000 bits per second running over the Controller Area Network (CAN) bus[223]
- OneNet describes a protocol using binary messages over the internet protocol (IP) version 6 and Ethernet at gigabit speeds, and introduces security mechanisms for transmissions[224]

The NMEA AIS protocols are used for inter-device communication aboard a vessel. NMEA 0183 has been adopted in ITU-R Rec. M.1371 for over-the-air transmission of AIS information.

The following example of a Type 1 (position report Class A) message demonstrates how AIS transmissions might appear to an AIS device. Suppose a device has the following information to send:

- MMSI = 367354360
- Navigation status = Underway using engine
- Rate of turn = 11.999° per minute to starboard
- Latitude = 41.3541750°
- Longitude = -072.0903817°
- Speed over ground = 5.21 knots
- Course over ground = 5.099°
- True heading = 17.000°
- UTC timestamp = 29 seconds

NMEA 0183-formatted messages are among the most common in use by commercial vessels, including some recreational and military vessels. NMEA 0183 messages are used for inter-device communication on a ship and have been adopted in International Telecommunication Union (ITU) Recommendation M.1371 for over the air transmission of AIS information. An NMEA 0183/ITU M.1371 message with the information above would be transmitted over the air as:

```
!AIVDM,1,1,,A,15NEQv02hlJmwiFGbKn@<hRr0000,0*43
```

NMEA 2000-formatted messages are used for inter-device communication aboard a ship. This standard is common on recreational vessels and those commercial and military vessels using modern AIS equipment. An NMEA 2000 message with the information above might appear as:

```
040EF801FF0289F811001C01F861E51577E107D57625A618757A030C0144C000970B2E1AC0F800
```

The OneNet standard is very new, and equipment employing this protocol is not expected to appear before the end of 2021. Like NMEA 2000, OneNet will be used for inter-device communication aboard a vessel.

Appendix 4. Malware Tutorial

An Introduction to Malware

Most common definitions of cybersecurity focus on the protection of computers, servers, networks, and the internet from deliberate attack and compromise.[225] The DOD definition of *cyberspace security* is much more global and focused:

> Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.[226]

The important distinction here is the focus on the bottom-line: information. Prior to the adoption of terms such as *cybersecurity* and *cyberspace security*, the practice was called *information security* or *information assurance*, providing the focus on the information itself rather than on the containers and communication pathways.[227] Textbooks today still talk about the so-called Confidentiality, Integrity and Availability Triad and Parkerian Hexad when describing characteristics of information, and there is a fair amount of overlap with the DOD terms:[228]

- **Confidentiality** refers to protecting information from unauthorized access or disclosure.
- **Integrity** refers to the state of information being free from inadvertent or deliberate manipulation.
- **Availability** refers to the users' ability to access information when needed.
- **Possession**, or control, refers to the loss of data by the authorized user (even if the "thief" cannot access the data).
- **Authenticity**, also known as authentication, refers to being able to prove the identity of the sender of information.
- **Utility** refers to the usefulness of the data to the user. Examples of low utility are possessing encrypted data without a decryption key; or receiving a message to do something after the date when the action is required.

The last part of the DOD definition, *nonrepudiation*, means that the owner of information or the sender of a message cannot deny their ownership or authorship, respectively.

Definitions of malware often focus on the intentional disruption to the operation of computers and communications systems, including user systems, servers, local networks, and the internet.[229] The real issue is that malware represents an attack on these characteristics of information; if we lose any one of these, the success of an operation or any data-based activity cannot be assured.

The use of malware and other attacks on computers and networks are tools commonly used by cybercriminals, cyberterrorists, and military information operators. Individual hackers and hacker groups can be acting for their own purposes, such as Anonymous; for hire, such as Lizard Squad, as state-sponsored actors, such as Syrian Electronic Army; or directly on behalf of a nation-state, such as People's Liberation Army [PLA] Unit 61398.

Malware Types and Techniques

There are many types of malware that manifest in different ways. Almost all malware is insinuated into a computer or network by a user opening an attached file to an email, downloading an infected file from an internet site, or otherwise responding to directions provided in a message from an "unknown" user. It is important to note that the term *computer* is a broad one; mobile devices such as tablets and cell phones are as susceptible to malware as a laptop or desktop system.[230]

Historically, malware has been categorized as a virus, worm, or Trojan. A *virus* is a nefarious program that is activated when executed by the user, such as when double-clicking on a file attachment to an e-mail. Once active, a virus can do almost anything on the system—slowly delete data; cause the computer's performance to degrade; make the computer part of a zombie network; or allow the system to become a jumping off point for another attack. Once installed, some viruses can automatically restart—even after they are discovered and closed, or the system rebooted. *Spyware* is a particular type of virus that collects keystrokes, contents of the system clipboard, screenshots, user logon credentials, and other information; it then uploads what it collects to an attacker's site. In one form or another, viruses have been infecting computers since the 1980s. In that era, the most common

form of distribution was via floppy disk software distribution or individual file sharing, and it could take months or years for a virus to hit a critical mass; by the early 1990s, commercial e-mail services and the internet greatly accelerated the time and ease for distribution.[231]

Worms can replicate and forward themselves to other systems. Worms use a variety of methods to propagate; one common method is to examine the e-mail address book of the infected system and forward itself to all addresses found therein. Another method is to advance via open network shares. Like viruses, worms can do just about anything to the host computer once they are active. Because of their ability to self-replicate, even a worm without a malicious payload can degrade the performance of a computer by usurping processing power, or of a network by consuming bandwidth. The concept of a worm has been around since the early days of the Advanced Research Projects Agency Network—the forerunner of the internet. The first worm to cause any sort of damage was The Internet Worm in 1988.[232] Worms are now the common way in which malware makes its way around the internet, and worm-based malware can hit critical mass on the internet within minutes or hours.[233]

Trojans, or *Trojan horses*, are programs that purport to do one thing but also contain additional, malicious functionality. Trojan horse software is often found as an e-mail attachment or Web site download, but there is also often some form of social engineering—manipulation of people—involved, such as someone on an e-mail list touting a new, wonderful game or application. Remote Access Trojans (RATs) are distributed by "customer service representatives," asking a user to download software so that the representative can share the screen with the user. These programs allow a bad actor to totally control the system. RATs and other Trojans are also distributed at some gaming, music sharing, and pornography Web sites where users are told to download special viewing software.[234] While Trojan software generally works as advertised, it also inserts additional malware which remains on the system even if the parent software is subsequently deleted; an example is CoinTicker, a Mac OS X application that monitors the current price of Bitcoin and other cryptocurrencies, and installs malicious backdoor programs that could allow an attacker to gain access to a user's cryptocurrency wallet.[235] Consider also ToTok, a messaging app introduced in 2019 that was downloaded millions of times by users around the world before being revealed to be a United Arab Emirates (UAE) intelligence service surveillance tool. Likewise, the smartphone video app TikTok was banned by branches

of the U.S. military because it was reportedly sending information back to its Chinese developer.[236] Trojans are a particular concern where operational systems have an internet connection, because the malware and its covert communications channels are totally hidden behind a useful facade.

Viruses and Trojans are pervasive on mobile devices, particularly the Android operating system. Mobile devices are an especially attractive target for attackers because of the incredible amount of personal information on those devices, including e-mail and text messages, photographs, financial and health information, logon credentials for a work network, and more. Information-stealing software is as likely to target mobile devices as it is personal computers.

Lastly, bogus hardware can also be employed as a vector with which to upload malware to a computing device. One such example is the O.MG cable, an Apple Lightning cable for charging an iPhone from a USB source. The USB connector on the O.MG cable contains an IEEE 802.11 Wi-Fi chip that allows an attacker to take control of the cable and, if the cable is connected to a Mac computer, provides the attacker an entry with which to exploit the Mac. The O.MG cable looks identical to the Apple USB Lightning cable.[237]

Phishing and Watering Hole Attacks

Phishing is a form of social engineering, whereby a message comes from what appears to be a legitimate source and asks users for some form of personal, sensitive information—such as name, address, social security or military identification card number, credit card information, or logon credentials. Phishing is fraud and uses trickery, manipulation, and, in some cases, intimidation, for its success. The goals of phishing are generally for an attacker to perpetrate some financial fraud or identity theft, but these same schemes can also be used for intellectual property theft, access to sensitive information, or intelligence gathering. Different forms of phishing can be used to achieve these myriad goals.[238]

"Traditional" phishing generally refers to attempted fraud by use of an e-mail containing an urgent message directing the user to a bogus, but legitimate looking Web site. The user is asked for all sorts of personal information and, upon submission, is typically redirected to the actual legitimate Web site. Users tricked by this scheme often do not realize that they entered data at a bogus site.[239]

Pharming is a more sophisticated form of phishing. Knowing that many users look in their browser's address bar to see if the web address of a page appears valid, attackers create a two-step attack. In the first step, the local Domain Name System (DNS)[240] name server is manipulated so that a legitimate website's name is associated with the bogus website's IP address.[241] In the second step, the user is directed to go to the website. At this point, even if the user types the address directly into the browser rather than click on the link, the correct address will appear in the address bar—although the displayed page will be at the bogus site.[242]

A *spear phishing* attack comprises messages specifically directed at individuals with some form of common interest, such as financial officers, employees who attended a meeting or class together, etc. Members of the military are often targeted by spear phishing attacks. For example, news of some activity is mentioned in the press or information about crew members of a vessel or team members of a group are somehow acquired by an adversary. Spear phishing messages can be highly personalized and made to be very convincing. *Whaling* is a variant of spear phishing, where messages are directed at senior executives, commanders, or other high-profile individuals within an organization or unit.[243]

Not all phishing comes via e-mail. *Vishing*, or voice phishing, is a phishing scam using the voice network, usually employing a synthesized voice because these are robot calls. Messages usually tell victims about some activity that requires that they provide their credit card or bank account number; ask for an immediate callback in order to pay off a non-existent bank debt; settle a tax judgment from the Internal Revenue Service; or avoid being arrested. On mobile phones, the caller's number is often spoofed so that it appears to come from the same area code as the target. Similarly, *smishing*, or short message service phishing, uses text messages as the vector for phishing.[244]

There are many common themes to phishing messages that cause individuals to provide their personal information, such as:

- there has been a compromise to a credit card or bank account
- there is a questionable purchase charged to your account
- respond to a bogus confirmation of a purchase
- notification of winning a sweepstakes, lottery, gift card, or other award
- an unsolicited job offer

- information required to continue benefits (e.g., Social Security), keep an account open, receive a tax credit, repair/validate a database, or avoid going to jail
- requesting information to authenticate your identity and confirm your continued availability on your local volunteer fire department, ambulance service, or reserve unit during times of imminent natural disaster or weather event

Although not a phishing attack, per se, *Watering Hole* attacks are a focused form of manipulation that target groups with a common interest. The attacker starts by gathering intelligence on the target victims to determine or observe what websites the group often frequents; for example, if the target victims go to the same sports or news website every morning. If the attacker cannot find such a website, a sophisticated adversary might create such a website specifically in order to attract the targets to one place.

The next step is for the attacker to somehow insert malware into the common website. Over time, the malware will infect susceptible user systems. As systems within the target organization get infected, the attacker can start to access information or otherwise manipulate the compromised targets. Even groups of users that are resistant to phishing and spearphishing will be victimized by watering hole attacks because of users' inherent trust in the security of websites.[245]

DoS/distributed denial-of-service (DDoS), Botnets, and Zombies

While traditional malware infects computer systems, there is another form of attack on the availability of information that can serve the purposes of an adversary: a DoS. The most secure network in the world with the best data is all for naught if no one can access the data.

DoS attacks generally succeed against their targets using a resource exhaustion strategy. Probably the first intentional internet DoS attack occurred in 1996 when someone started flooding Panix—one of the oldest internet service providers in the world—with 150 packets per second (70 kilobits per second) of connection requests that were intentionally never completed. In this way, Panix servers allocated all their memory buffers to pending connections, which effectively blocked new connections from being created.[246] It was not technically difficult to launch this attack, yet it was so new at the time that Panix was down for several days while a defense was

mounted. In 2005, another DoS was launched against Panix when someone hijacked their domain name, disrupting access to their network for a couple of days.[247]

Another form of a DoS attack is to flood the victim's website with enough data to consume all the bandwidth on the internet connection. While a viable form of attack, it only works if the attacker has more bandwidth than the target.

A problem with any form of DoS, from the attacker's perspective, is that the source of the data packets can be traced back to the originator and attribution accurately made. In 1999, the first DDoS attack was used to disable the computer network at the University of Minnesota for two days.[248] In a DDoS, hundreds or thousands of computers are compromised with malware that puts them under control of the attacker; these systems are often called *daemons* or *zombies* and the collection of these systems is called a *botnet*. When the attacker wishes to launch one form or another of DoS on a victim, a message is sent to the compromised systems directing them to send their DoS payload to the victim site. The combined bandwidth of all the zombies is sure to exceed that of the victim site; two of the largest DDoS attacks to date occurred within days of each other, in 2018, when GitHub was flooded with data rates of up to 1.35 terabits per second (Tbps), and Arbor Networks was flooded with up to 1.7 Tbps.[249]

The GitHub and Arbor Networks DDoS are worth examining more closely, as they may represent a harbinger of things to come. These DDoS attacks employed a method known as *broadcast amplification*, exploiting a weakness in software known as *memcached*. The memory caching daemon or service on Linux, Unix, and Windows servers is used to cache, or temporarily store, data in memory in order to speed up processing on large data stores—such as disks and databases—and is commonly employed in cloud-based services to reduce response time.[250] Because memcached does not employ authentication, an attacker can send a message to one or more memcached servers while spoofing the IP address of the intended victim; in these cases, GitHub and Arbor Networks. An attacker can cause a small amount of data sent to the target server(s) to be amplified tens of thousands of times when forwarded to the victim; in this attack, a single 203-byte request resulted in a 100 megabyte[251] response. While patches for this vulnerability are available, studies estimated that there were more than 100,000 known, unpatched memcached servers on the internet in late 2018. If a nation-state wanted to

use this form of attack, they could, presumably, leave unpatched servers on the internet just for this purpose.

One of the biggest dangers from DDoS attacks is that the attacker does not need to have any special access to the target victim's network to cause a disruption or outright blockage. Thus, any operational network is at risk of this type of attack by an organized adversary. While there are manual and automatic methods to mitigate the impact of a DDoS attack, there is always a time lag between the initiation of an attack and the ability of the network to respond and adapt. A DoS attack can be timed in such a way as to coincide with a kinetic event, either as part of an offensive or defensive action.

Ransomware

Ransomware is a form of malware that, as the name implies, locks a user out of a computer system unless the user pays a ransom. While the first form of malware extortion is thought to be the AIDS Trojan in 1989, modern forms of ransomware have been around since about 2012; it has been one of the top forms of cyber malware since about 2016.

Figure 16. Screen shot is shown of WannaCry ransomware. Source: Wikimedia Commons CC BY-SA 4.0

Ransomware can be distributed as a virus or worm and can target traditional computer systems as well as mobile devices. The ransomware will

generally encrypt the system's files or otherwise make the system inaccessible to the user, and then demand ransom for the user to recover the decryption key (figure 16). In most cases, the ransom demand requires payment of a certain amount of money within a few days, then doubles for a few more days, and then expires; this gives users little time to try any decryption efforts, which generally will fail. Payments are commonly made by anonymous cryptocurrencies, such as Bitcoin or Monero. In most cases, the decryption key is delivered to the victim upon payment because distribution of ransomware is generally a criminal endeavor and the attacker just wants the money; if word got out that the key was not distributed, other victims would not pay the ransom. Note that many forms of ransomware have a help line for the victim to learn how to create a cryptocurrency wallet and transfer funds. An alternative form of ransomware is where an attacker downloads sensitive files and threatens to release them unless a ransom is paid.[252]

Figure 17. Ransom demand as part of *memcached* attack payload is shown. Source: Brian Krebs/used with permission

Nothing limits ransomware to cybercriminals and opportunistic crime. Consider the memcached DDoS attack described previously. The payload in some versions of the memcached attack include a ransom note repeated over and over; figure 17 shows a demand for 50 Monero cryptocurrency that can be paid to the address shown in the message.[253]

Ransomware is increasingly used to target health care, financial, and public sector sites around the world. More than 200 local and state municipalities have been targeted in the U.S. since 2013, in such locations as Albany, Atlanta, Baltimore, Cleveland, Detroit, Las Vegas, Riviera Beach Florida,

and San Antonio; indeed, 22 cities in Texas were hit in a single attack in 2019. Nearly 50 U.S. local and state law enforcement agencies have also been victimized.[254] A common thread of these attacks is that—due largely to a lack of comprehensive disaster recovery and business continuity plans—their operations ground to a halt, employees lost internet and e-mail access, departments had to resort to pen and paper, and records were lost.

There is little question that ransomware will continue to be used as a cyberweapon of nation-states and cybercriminals. The problem will undoubtedly get worse with increased deployment of IoT and smart devices. Hackers selling ransomware-as-a-service will make these types of attacks easier, more organized, and more prevalent by any number of bad actors.[255]

APTs

APTs refers to a cyberthreat that targets a specific organization or sector and combines all the tools in the hacking toolkit—from social engineering and exploiting vulnerabilities to phishing and distributing malware. While the attack might be deflected for a while, the attacker does not go away.[256]

APTs are so named because each word offers a characteristic of the type of attack:[257]

- **Advanced.** Attackers use a broad array of tactics, techniques, and procedures (TTPs), employing commercial, open source, and their own private computer and network intrusion tools; the methodology is advanced even if the individual tools are not.
- **Persistent.** These attacks are targeted rather than opportunistic; they generally employ low-and-slow techniques to avoid detection. The goal is long-term access rather than short-term disruption.
- **Threat.** APT actors have the capability and intent to do harm, generally being coordinated actions sponsored by nation-states or highly organized groups.

The APT term was coined in early 2010 related to an event called Operation Aurora. During the latter half of 2009, Google and reportedly dozens of other organizations—including Adobe Systems, Juniper Networks, Northrop Grumman, Symantec, and Yahoo!—were targeted by the Chinese PLA Unit 61398.[258] Google claimed that intellectual property had been stolen and accounts of Chinese dissidents targeted. The attack exploited a vulnerability in Internet Explorer that had been reported to Microsoft in September

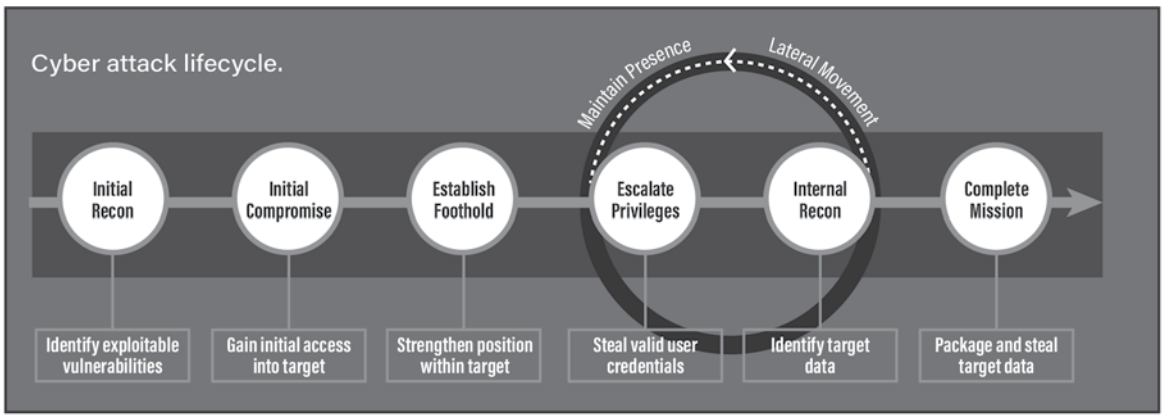


Figure 18. Mandiant's APT attack lifecycle model is shown. Source: Jurgen Kutscher, "M-Trends 2017–A View from the Front Lines," *FireEye*/used with permission

2009, but not yet patched. As a result of this attack, Google closed its Chinese operation.[259]

As suggested in figure 18, an APT is organized and focused. According to early analysis of Operation Aurora by Mandiant, there are several distinct phases in the attack; although this model had been modified over time, the basics still hold:[260]

- **Initial Reconnaissance.** Using public information sources, the attacker identifies potential targets by learning about the organizational structure, key individuals, servers, the network architecture, network services and possible vulnerabilities, and other information posted at the organizational website or social media.
- **Initial Compromise.** Using TTPs such as social engineering, phishing, or exploiting a vulnerability on a server system, the attacker inserts some malicious code that provides an entrée into the network.
- **Establish Foothold.** Once in, the attacker ensures continued access to the compromised system by creating a hidden account for themselves or installing additional utilities or malware.
- **Escalate Privileges.** Further exploitation of the compromised system yields the attacker a higher level of privilege, allowing greater access to systems and data.
- **Internal Reconnaissance.** Now on the inside of the target network, the attacker can gain a better understanding of the environment, which individuals provide the best route to additional data and the location of key databases and control systems.
- **Lateral Movement.** Having identified other target computers within the network, the attacker uses their privilege to move from system to system via network shares or remote access tools and services.
- **Maintain Presence.** Once an attacker moves on to a new system, they can use it to continue learning about the compromised network environment and to ensure continued access to the environment—even if their presence is detected on another system. Again, the use of malware, backdoors, remote access software, and virtual private network software might be employed.
- **Complete Mission.** Once the attacker accomplishes their goal—be it to steal intellectual property, operational plans, organizational information, logistics and personnel information, personally identifiable

information, or other data—they often allow the active operation to go dormant, but they leave their access intact in case they wish to come back later.

APTs are an insidious attack, rarely showing signs of hostile activity in their early stages. If invoked by a nation-state, these actions are in furtherance of long-term goals; indeed, tomorrow's adversary might already be preparing today with APT planning.

Zero-day Exploits

All malware leverages vulnerabilities in software. Software vendors generally fix vulnerabilities as they are discovered, but the sheer volume of program errors mean that the vendors must prioritize which flaws get patched and which ones do not during any given patch cycle. Generally, the most serious get fixed the soonest; some flaws remain for months or years while others never rise to a level serious enough to get fixed, unless or until they are actually exploited.

The term *zero-day exploit* is applied to malware that exploits a vulnerability that either was unknown or not patched before the malware struck. In either case, the immediate consequence is that there is no short-term defense while victims try to gain situational awareness to understand what is happening.[261] Operation Aurora, described previously, is a perfect example. The attackers against Google and others started in mid-2009 via the exploit of a previously unknown Internet Explorer vulnerability. Microsoft became aware of the vulnerability in September 2009 but did not create a patch for another month or two. The attack against Google essentially ended in December but was not publicized until January 2010.[262]

Zero-days have been stockpiled by any number of groups engaging in offensive information operations, largely sponsored by nation-states. These groups look for obscure vulnerabilities specifically to weaponize the exploit; these have become tactical assets to use in strategic cyberattacks, since they can only be used once to temporarily disrupt an adversary. Most major software vendors have bug bounty programs, paying individuals to find major flaws in their software; some people will sell vulnerabilities they find to the highest bidder—or, in some cases, to multiple bidders.[263]

Perhaps the most public demonstration of the weaponization of zero-day exploits is the NSA/CIA Toolkit. In 2016, a hacker group called The Shadow

Brokers announced that they possessed a set of cyberattack tools developed by the NSA and CIA—including several zero-days that target a wide range of systems. The Shadow Brokers released the first set of files, called Vault 7, to WikiLeaks in March 2017 and, subsequently, nearly two dozen more sets of files were released over the next six months. The tools included hacks and zero-day exploits for all major operating systems, Society for Worldwide Interbank Financial Telecommunication (SWIFT) applications, smart televisions and other IoT devices, and many types of routers.[264]

Appendix 5. CPS Tutorial

OT and ICS and IoT, oh my![265]

CPS refers to the engineering problem of merging the physical and cyber worlds. There are a lot of terms and concepts used when talking about CPS that all appear to describe the same things, and that will be the focus of this section.[266]

OT is an umbrella term that encompasses the various technologies that enable the cyber and physical worlds to come together (figure 19). OT systems are those where computers directly interact with physical processes by near-real-time monitoring and/or control of physical devices such as valves, pumps, production lines, the power grid, dams, transportation systems, and much more.[267]

ICS represent a major segment within the OT sector and is composed of systems used to monitor and control industrial processes, such as factory

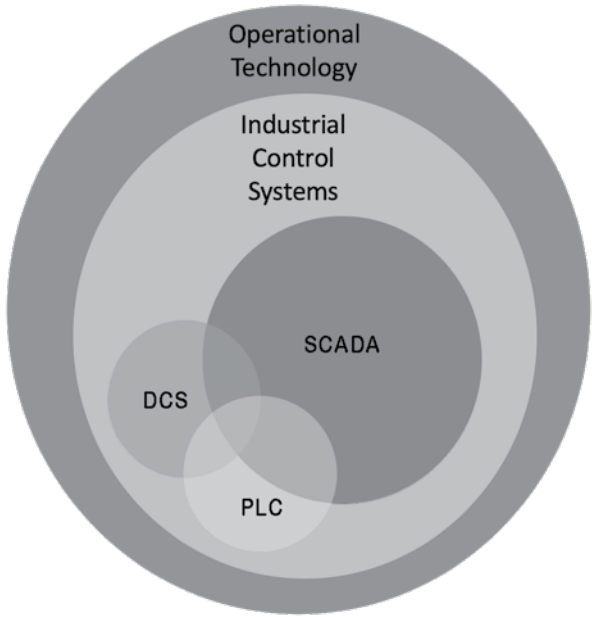


Figure 19. The components of CPS and the IoT are shown. Source: Gary C. Kessler

floor automation, power consumption management of electricity grids, wind farm controls, or vessel management systems. ICS specifically refers to computing systems used to manage industrial operations and other CPS applications as opposed to the more common ICT systems that manage administrative operations; put another way, ICS controls the physical world and ICT systems manage data.[268]

The requirements of ICS software and hardware in an operational environment are quite different than those of ICT systems in a normal business environment. These differences are primarily found in the characteristics of performance, system reliability, and security priorities. As seen in table 4, ICS applications require real-time, low-delay, high-availability hardware and software. Because of these requirements and the large number of installed systems, the components need to be thoroughly tested prior to deployment. Indeed, some of the embedded ICSs are used as part of licensed or regulated systems, so that any updates and modifications require certification by some authorizing agency. The implications of system failure—or security vulnerabilities—can also be catastrophic well beyond the device itself, potentially threatening the environment, safety to people or equipment, or the business unit's very future.[269]

Table 4. Requirements for ICT and ICS. Adapted from: NIST SP 800-82, 2015

ICT	ICS
Performance	
Non real-time	Real-time
Response must be reliable	Response is time-critical
High throughput required	Modest throughput accepted
High delay and jitter accepted	Requires low delay and jitter
Reliability	
Scheduled operation	Continuous operation (24/7/365)
Occasional failures tolerated	Outages intolerable
Beta testing in field acceptable	Thorough testing prior to deployment
Modifications possible with little paperwork	Formal certification of changes often required
Security Priorities	
Risk Impact: Loss of data confidentiality, integrity and availability; business operations	*Risk Impact*: Environmental, safety, business operations
Recover by rebooting	Fault-tolerance/redundancy essential

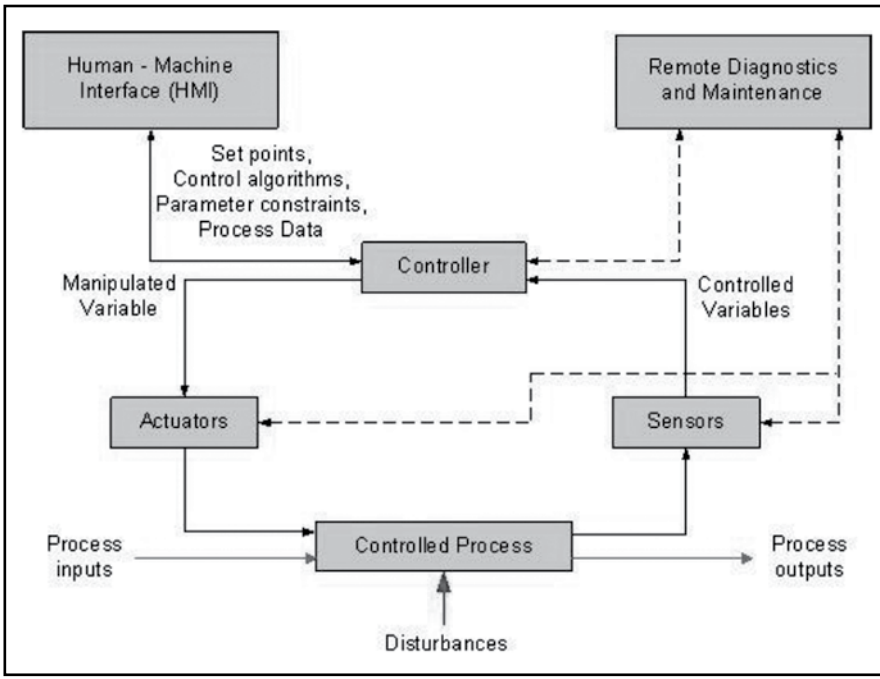


Figure 20. ICS operation. Source: NIST SP 800-82

Figure 20 shows the architecture of a generic ICS. The core of the system itself is generally the feedback loop composed of sensors, controllers, and actuators that manage some controlled process. The *sensor* measures some physical property and sends this information as a set of variables to the controller. The *controller*, in turn, interprets the signals and generates appropriate instructions, based upon some control algorithm and desired set points, which are sent to actuators. Based on the controller's instructions, *actuators* directly manipulate the controlled process via control valves, breakers, switches, motors, and other physical devices. Much of this activity can be automated since a human might not be able to respond as quickly as the system's changing state demands. Indeed, the human-machine interface (HMI) is generally for high-level functions such as setting and adjusting operational parameters for the controller, monitoring system activity, displaying status information, and reviewing system history rather than for moment-by-moment system control. Diagnostics and maintenance utilities also provide overall monitoring of the system to prevent, detect, and respond to abnormal operation or failures.[270]

A complete discussion of the myriad uses for ICS is beyond the scope of this monograph, but suffice to say that such systems vary widely in their feedback loop timing and response time requirements, geographic distribution, fault tolerance, control complexity, architecture, redundancy, and impact upon failure.[271] Further discussion of ICS will focus on information relevant to maritime applications.

ICS include a variety of control system configurations, including programmable logic controllers (PLC), distributed control systems (DCS), and supervisory control and data acquisition (SCADA) systems. A PLC, at its heart, is merely a special purpose—often ruggedized—computer used to control hardware devices in an industrial automation environment. The PLC might be realized as a controller board interface in a computer or, built as a specialized piece of hardware; in either case, the PLC receives data from sensors and other input devices, processes the data per some preprogrammed algorithm, and sends control data to the hardware devices being managed. The PLC might be a stand-alone device with its own HMI display/keyboard, or part of a distributed network of PLCs communicating to some central controller.[272]

A DCS is a control system for some process that generally includes many feedback loops distributed amongst many computerized controllers, without a central management system. A DCS might be built as a set of networked PLCs, each autonomous but reporting back to a central operator's HMI station; it is the DCS that provides the logic of the distributed system and the PLCs are the subsystems that implement the control function.[273]

Shipboard automation employs ICS, SCADA, and other CPS/IoT standard communications models. The automated systems employ an HMI with monitors, keyboards, joysticks, touchscreen panels, etc.; a controlling or supervisory computer; PLCs to control the hardware valves, switches, motors, and other hardware; and a communications network connecting the various components, primarily using NMEA standards over serial lines, the CAN bus, Ethernet, wireless, or other media.

SCADA systems provide a central management platform from which operators can monitor, manage, and maintain situational awareness about a distributed ICS. SCADA systems integrate data communications, a graphical HMI, and data acquisition capabilities so that operators can easily observe the status of the system, quickly detect abnormal activity or system status,

and intuitively adjust managed processes. The primary components of SCADA systems are:[274]

- SCADA display unit, a graphic display HMI showing status messages and alarms.
- Remote terminal units (RTUs), often geographically dispersed from the central control station but close to the process being managed or monitored; a PLC or DCS can act as an RTU.
- A control unit attaches the RTU to the SCADA system, passing data between the RTU and central controller in real-time with low latency.
- Communication links, ranging from high-speed local Ethernet to wide-area leased lines or radio.

DCS and SCADA are similar systems but there are a couple of important differences. First, SCADA assumes a central management point whereas DCS does not. Second, DCS is process-driven, meaning that it operates sequentially step-by-step, implements the programmed processes, and responds to inputs by its controller when necessary; SCADA systems are event-driven, meaning that the system waits for an event to occur that requires an action. Finally, DCS is intended for a system distributed over a relatively small geographic area; SCADA is designed for exceptionally large geographic areas.[275]

CPS and IoT Cybersecurity Issues

A typical CPS consists of two primary components—physical devices, and computers where the computers monitor and/or control the physical devices. Where there are computers, there are cyber vulnerabilities and the computer processors that comprise CPS and IoT networks are no exception. ICS are complex systems prone to vulnerabilities that can be due to the system architecture and design, user policies, configuration and maintenance policies and procedures, the physical system, software development, and the communication and network configuration. Threats can also come from many sources including adversarial threat actors; accidental actions by users; structural failures of equipment, controls, or software; or environmental failures due to natural disaster, man-made disaster, or external infrastructure failure outside the control of the system. These threats affect CPS and IoT across all critical infrastructure sectors, including healthcare, telecommunications, agriculture, energy, and transportation.[276] A complete overview of

cybersecurity threats in this domain is beyond the scope of this monograph, but a few examples will suffice to demonstrate some of the issues.

While common malware directly attacks computer systems, there are variants that target hardware via their computer controllers. One of the first demonstrations of a software attack on hardware was the Aurora Generator Test conducted by the U.S. Department of Homeland Security in 2007.[277] Generators, motors, and other components in many critical infrastructure sectors—including energy, transportation, oil and gas, and water—employ digital protective relays that control circuit breakers. These relays ensure that the hardware remains synchronized and functions within proper operational parameters. The Aurora test was a controlled hack into a 27-ton generator's control system, where relays were disabled, thus holding circuit breakers open for an amount of time sufficient for the machine to slip out of sync and subsequently vibrate so violently that it broke itself apart. The test required less than three minutes to be successful.[278]

Possibly the first malware in the wild known to attack hardware was Stuxnet, a Microsoft Windows-based worm that was discovered in 2010. The Stuxnet worm employed several zero-days exploits and targeted a particular type of Siemens centrifuge known to be used at Iranian uranium enrichment facilities. The worm was believed to be initially introduced by USB thumb drives but also propagated via local networks and, presumably, the internet. First, the malware targeted only Windows systems. Once on such a system, it checked for the presence of Siemens Step 7 software, the Windows software that managed the ICS for the centrifuges. If it found that software, Stuxnet then compromised the PLCs, accelerating the centrifuges to such a high speed that they broke apart, all the time showing "normal operation" on the HMI displays. One of the many lessons of Stuxnet is that it is impossible to control a malware weapon in the wild; while Iran was the target, only about 59 percent of the victim systems were located in Iran.[279] Stuxnet was followed by more weaponized malware with names such as Duqu, Flame, and Gauss. Inevitably, there are families of malware that specifically target ICS, such as CrashOverride and Trisis/Triton, both of which appear to target power grids and utility systems.[280]

ICS provide an opportunity to build systems that can respond to abnormal events faster and more efficiently than a human. But these systems need to be understood by the humans who manage them and, indeed, must provide a way for the human to override the automatic controls should they be

compromised. Although not a cyber issue, per se, issues with the Boeing 737 MAX 8 provide an object lesson. The 737 MAX is equipped with an automatic trim system called the Maneuvering Characteristics Automation System (MCAS). A larger engine on the 737 MAX caused the plane's stability characteristics to be different than on previous versions of the 737 and, in fact, harder for the pilots to fully manage. MCAS was meant to better control the handling of the aircraft by monitoring an angle of attack (AOA) sensor. However, in two crashes of the 737 MAX, the system overcorrected, and the pilots could not override the system. In the crash of Ethiopian Airlines Flight 302, the AOA sensors provided erroneous readings causing the plane to deviate from a smooth take off. Pilots attempted to regain control, but the MCAS would then take over again; it appears that the pilots and MCAS exchanged control of the plane several times during its six-minute flight.[281]

As noted above, there are billions of IoT devices globally on the internet and many are not well secured. These devices are an attractive target for an attacker because they represent incredible computing power as a distributed network or botnet. The botnet, in turn, can be used as a platform with which to launch DDoS attacks with incredible bandwidth against their victims. Due to a desire to keep prices down, IoT devices are largely designed to depend upon the border security of the network on which they are installed, leaving the devices themselves prone to weaknesses ranging from insecure web, mobile, or cloud accessible interfaces, inadequate tools with which to configure security parameters, and insecure software or firmware to weak authentication/authorization mechanisms, insecure network services, and a lack of encryption. The IoT networks themselves have many points of insecurity, including the sensors, communications network, and the back-end IT systems. While these are generic IoT security concerns, each specific application and architecture introduces its own security issues.[282]

The threat of IoT device exploitation is so real that the Federal Bureau of Investigation (FBI) released a public warning about potential exploitation as far back as 2017.[283] And the FBI's warnings were well warranted. There are sites on the internet that allow people to search the internet for IoT devices,[284] and other sites where people can find known or leaked passwords for IoT devices.[285]

Due to these weaknesses and vulnerabilities, IoT devices have been compromised and used as part of several large DDoS attacks. One of the best known was the 21 October 2016 attack against Dyn, a company providing

internet performance management, name registration, and DNS services. The Dyn attackers used malware called Mirai, which targeted Linux systems—a common operating system on IoT processors—and primarily focused on consumer IoT equipment, such as remote cameras and home routers. The Dyn DDoS employed a botnet of tens of thousands of compromised IoT devices, sending an estimated load of up to 1.2 Tbps. Dyn hosts websites for more than 70 major media, news, commercial, financial, communication, and other organizations; all were inaccessible for most of a day while Dyn suffered from three waves of DDoS. While Anonymous and New World Hackers claimed responsibility for the attack as retaliation for the Ecuadorian embassy in London rescinding Julian Assange's[286] internet access, others have claimed the attack was perpetrated by script kiddies or an angry gamer. The real bottom line is that the attack was not technically complicated and well within the means of almost any hacker.[287] IoT botnets using the Mirai malware were also used to perpetrate DDoS attacks a month earlier against the KrebsOnSecurity blog (600 gigabits per second) and OVH, France's largest web host (1.1 Tbps).[288]

Appendix 6. Autonomous Vessel Background

Drivers for Autonomous Vessels

The maritime industry has been engaging in research and planning for the likely adoption of autonomous vessels for many years. OT and IoT technologies have caught up to the demand so that such vessels are becoming a reality. Given this, *autonomous* can mean different things to different people; it is used to refer to highly automated vessels with skeleton crews, remote-controlled vessels, fully autonomous/unmanned vessels, and hybrids that are some combination of all of these.[289] While most of the work on autonomous vessels is driven by economic imperatives, practical requirements are also at play. As an example, due to the travel restrictions brought on by the 2019 Coronavirus disease, Royal Caribbean's Silversea Cruises conducted remote control testing during the April 2020 sea trial of a new vessel, *Silver Origin*. The captain, on board, acted as lookout while the maneuvering systems were controlled and calibrated by an operator 1,120 miles (1,800 kilometers) away.[290]

For purposes of the discussion in the remainder of this appendix, *autonomy* will refer to fully autonomous or hybrid remote-control/partially autonomous vessels that do not have a crew on board.[291]

There are myriad factors that make autonomous vessels attractive to the industry. One of the biggest is safety; the majority of maritime accidents are caused by human error and a large number of those errors are due to fatigue.[292] Autonomous vessels with automated controls and responses, possibly including a remote operator, will presumably be able to remain alert on a 24/7 basis and respond more quickly than humans to unexpected events.[293] Vessels can be designed that will carry more cargo than today's cargo vessels because they will not need space for people-oriented structures such as decks, a bridge, and crew quarters, nor will they need environmental systems that would support a crew. As a result, these ships can be designed to be more wind resistant and streamlined in the water (figure 21), resulting in a lighter, more efficient vessel that will be cheaper to operate and use less fuel.[294]

Autonomous vessels also offer a response to the problem of finding and attracting trained merchant mariners for the growing commercial fleets. As

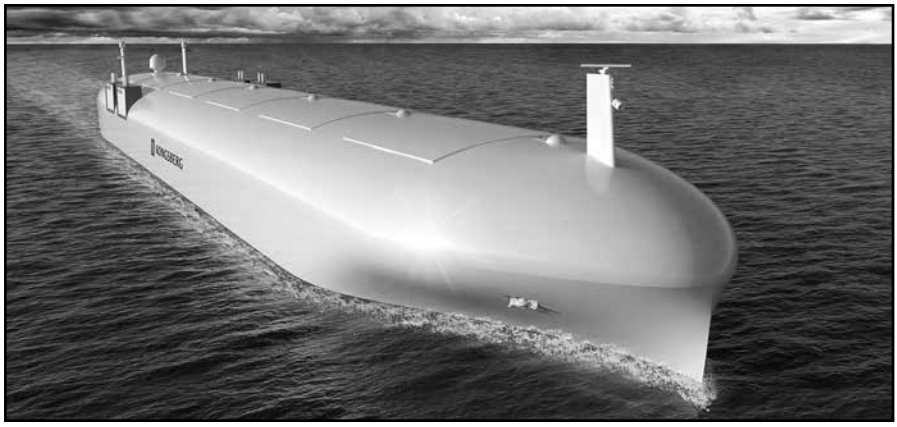


Figure 21. Rendering of an autonomous cargo vessel at sea. Source: Kongsberg Maritime/used with permission

ships become more and more dependent on computers and other automation, shipping lines are finding it increasingly difficult to find merchant mariners with the necessary maritime and technical skills to operate a modern vessel. At the same time, fewer people from developed nations are looking to the merchant marine as an attractive career, given the long times at sea away from friends and family. Indeed, unmanned vessels might also be less prone to the dangers of piracy due to the fact that there are no hostages to take.[295]

Without a human on board, a ship's automated controls and/or remote operator will be dependent upon numerous technologies. Situational awareness and PNT functions will still require GNSS fixes, weather reports, AIS, and other communications from other vessels and shore stations. High-definition visible-light and infrared cameras, radar, and lidar will supplement these systems by providing a broad picture of the local environment. These systems become critical when operating in the LZ due to the relative congestion of shipping, localized hazards, and rapid rate of a changing conditions in these waters.[296] Autonomous vessels operating inland, near-shore, or near congested shipping lanes require far more diligence and attention on the part of the ship's master or operator yet the technology systems on which they must depend have many cybersecurity vulnerabilities, as discussed in previous chapters.

While advantageous for many reasons, autonomous vessels will also require operational changes, particularly when an autonomous vessel is

around other ships—which will have a heightened impact on operations in the LZ. The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers is designed for mariners at sea and neither for autonomous vessels nor mariners operating from a shore station.[297] In addition, maritime rules of the road are designed for manned vessels; how, for example, should an autonomous vessel meet the lookout requirement in Rule 5 of the 1972 Convention on the International Regulations for Preventing Collisions at Sea?[298]

Autonomous vessel-related research is one of the most active areas within the maritime sector.[299] It is likely that full autonomy will start with services in the inshore or near-shore LZ, such as short haul ferries, autonomous tugboats, and autonomous offshore mooring systems. Autonomous military vessels are already being considered for some routine operations and integration into battle groups. Autonomous drones will undoubtedly be integrated into near-shore and inland vessel and port operations, along with autonomous vehicles at the ports themselves.[300] All of this raises the specter of another USS *Cole*-like attack occurring in a foreign port with swarms of automated vessels, drones, or other vehicles.[301]

Autonomous Vessels in the MTS

The 2010–2020 timeframe saw many research and development initiatives around MASS, including:

- The European Commission's Maritime Unmanned Navigation through Intelligence in Networks project ran from 2012–2015 and addressed operational, technical, and legal aspects of autonomous shipping.[302]
- Rolls-Royce has been an industry leader in MASS research, leading the Advanced Autonomous Waterborne Applications (AAWA) Initiative from 2015 to 2017, with plans for rollout of a small vessel in the early 2020s. The follow-on project, called Safer Vessel with Autonomous Navigation (SVAN), focuses on implementing the lessons learned from the AAWA project.[303]
- Mitsui O.S.K. Lines and Mitsui Engineering & Shipbuilding were selected, in 2017, by the Japanese government to lead the development of an autonomous ocean transport system.[304]

- The Novel Inland Water Transport and Maritime Transport Concepts project is promoting the vessel train concept, where a fully crewed vessel leads a group of semi-autonomous vessels, all of which are in communication with the lead ship. Funded by the European Commission in 2017, the research involves 22 companies from nine countries.[305]
- In 2018, Norwegian shipping companies Kongsberg and Wilhelmsen established a joint venture called Massterly, with plans to offer the complete suite of autonomous vessel services including design, development, control systems, logistics, and operations.[306]
- In 2019, the Maritime and Port Authority of Singapore launched their Maritime Innovation Lab to start research and development of several autonomous maritime programs—including vessels, navigation systems, and situational awareness systems.[307]

The era is upon us when research leads to the nascent stages of autonomous vessel implementation. In December 2018, Rolls-Royce[308] and Finferries demonstrated the first fully autonomous transit and docking of a vessel with *Falco*, a 177-foot (53.8 meter) car ferry in Finland (figure 22). Using results of the SVAN project, *Falco* operated in a fully autonomous mode on the one mile (1664 meter) outbound trip and under remote control on the return; a captain monitored the vessel from an autonomous operations center 30 miles (50 kilometers) away.[309]

Figure 22. Demonstration of the first fully autonomous transit and docking of a vessel, using the car ferry *Falco*. Source: Finferries/used with permission

In February 2020, Bastø Fosen, Kongsberg, and the Norwegian Maritime Authority started a six-month trial running *Bastø Fosen VI*, a 469-foot (142.9 meter) semi-autonomous passenger and vehicle ferry, on an approximately seven mile (11 kilometer), 30 minute route. Dubbed the world's first adaptive ferry transit, the vessel operates under fully automated control from dock to dock, with a captain and full crew on board for oversight.[310] In another project, Kongsberg and Yara plan to have *Yara Birkeland*—a 260-foot (80 meter) electric, autonomous container ship—operational by 2022. This vessel will transport cargo on an approximately 15 mile (24 kilometer) inland route in Norway.[311]

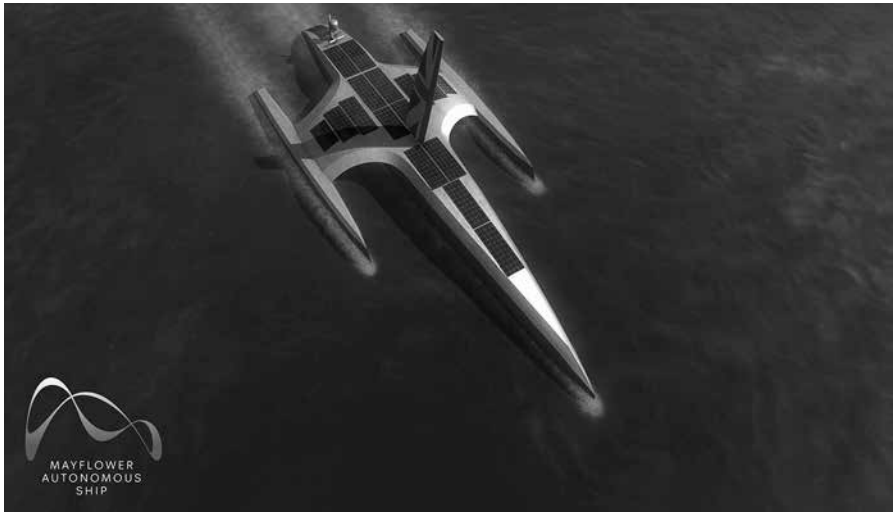


Figure 23. Rendering of the autonomous vessel *Mayflower*. Source: IBM/ProMare/ used with permission

September 2020 was the 400th anniversary of the Pilgrims departing England on the sailing vessel *Mayflower*. The fully autonomous vessel *Mayflower* is scheduled to start the 3,220-mile (5,182 kilometer) trip from Plymouth, England to Plymouth, Massachusetts in May 2021 (figure 23). The Mayflower Autonomous Ship (MAS) project is a global consortium that includes IBM, ProMare, the University of Birmingham UK, and the University of Plymouth UK. *Mayflower* will rely on solar, diesel, and wind power, and will employ AI, deep learning, and standard maritime technologies to manage the crossing. This will represent the first trial of a full-sized, open ocean autonomous vessel.[312]

Large autonomous cargo vessels as envisioned by the industry will necessarily change the way in which those ships interact with tugs. As might be expected, research into the use and deployment of fully autonomous and/or remote-controlled tugboats is an area of extensive research. Appropriate autonomy technology might vary whether the tug will operate in ports and port approaches (harbor tug); at offshore terminals (terminal tug); as an escort for tankers, gas carriers, bulk carriers, or large container vessels at a relatively high speed in port approaches (escort tug); or as an emergency towing vessel. Autonomous operation of tugs is challenging for many reasons, not the least of which is the way in which two ships affect each other when in proximity at sea. Given the fact that the tug will be the smaller of the two vessels, it is the tug that has the higher risk. Indeed, proper use of AI and ML is as high a priority with tugs as is autonomous controls and navigation. Maneuvering the tug—or a set of tugs—is only the first step; now the tug needs to connect to the larger vessel. Autonomous tugboat-ship coupling systems is another area that needs to be developed.[313] Tests of autonomous and remote operated tugs have been underway since 2017 in the North Sea, Port of Copenhagen, Port of Singapore, and other areas around the globe; although most have been under relatively optimal conditions, tests in adverse weather and seas has not yet been performed.[314]

Another area of research in this sector is autonomous mooring systems, both in port and at offshore facilities. Autonomous mooring systems can be used with any type of vessel but have some obvious advantages for autonomous ships; as an example, one such system is being designed specifically for the *Yara Birkeland* to provide autonomous mooring as well as autonomous cargo loading and unloading.[315]

Although developed independently, autonomous unmanned aerial vehicles (UAVs)—or *drones*—have become a part of autonomous maritime systems. Both autonomous and remote-control UAVs have been proposed as aerial surveillance systems to provide additional collision avoidance information and a larger situation awareness perimeter to manned and autonomous ships.[316] Autonomous drones have also been proposed to supplement humans in ship inspections. Drones can safely enter locations on vessels that might be too dangerous for people—doing everything from transmitting a video feed for real-time analysis by an inspector or specialized software, to using high-spectral imaging for detailed analysis beyond the capabilities of a human.[317] Autonomous tugboats and mooring systems might also be

supplemented by autonomous UAVs for functions such as transporting heaving lines from the dock or tug to a ship.[318] All of these functions are likely to occur in near coastal or inland waters, meaning that mariners are likely to see more drones in the air, with no real a priori knowledge of their purpose or intentions. While remote-controlled and autonomous UAVs have some unique cybersecurity vulnerabilities, they are generically similar to those in the maritime space.[319] Further discussion of cybersecurity issues of UAVs is beyond the scope of this monograph.

Appendix 7. Approaches to Qualitative Risk Assessment

There are two primary methods in which to perform cyber risk assessment: *quantitative* and *qualitative*. Quantitative methods are objective and measurable, while a qualitative approach is more subjective and less tangible. Quantitative methods require the ability to assign value to assets at risk, which can include the cost of replacement, downtime, repair, negative publicity, etc. These methods also require the ability to predict the frequency with which assets will suffer loss. This allows the owner to do a cost-benefit analysis of the actual cost of cyber defense mechanisms versus the anticipated cost of asset loss. The major drawback of this method is that it takes a long time to do this analysis well, even though it is extremely difficult to truly know the costs.[320]

Qualitative methods are scenario-based and work by describing the events that can go wrong. The assessor can then assign a "grade" based upon the perceived likelihood of an event occurring and the impact to the system or organization should the event occur. This type of planning helps an organization identify strengths and vulnerabilities to create contingency plans and recovery systems. In the most common usage, the probability of occurrence is a five-point scale ranging from rare to certainty; severity is a four-point scale ranging from negligible impact to catastrophic (figure 24). Scenarios considered to be unlikely or that would rarely occur with a negligible or moderate impact fall into the low level of risk category, which is numbered four. Scenarios classified with higher likelihoods and/or higher levels of severity are placed into different risk categories with extremely high level of risk being the highest, which is numbered one. It is impossible to eliminate risk, but this qualitative tool assists cyber defenders in identifying the areas of most vulnerability and in prioritizing allocation of cyber defense resources to mitigate risk where possible.[321]

Chapter 5 introduced Tam and Jones' multi-axis model for autonomous vessel risk assessment.[322] It is a model that focuses on offensive strategy rather than defensive and could be applied to other aspects of maritime, or even more general, cybersecurity. Tam and Jones describe three axes, namely technology (i.e., level of autonomy), attacker reward, and ease of exploit.

RISK ASSESSMENT MATRIX				PROBABILTY Likelihood of Mishap if Hazard is Present				
				A Almost Certain (continuously experienced)	B Likely (will occur frequently)	C Possible (will occur several times)	D Unlikely (remotely possible but not probable)	E Rare (improbable; but has occurred in the past)
SEVERITY Consequence if Mishap Occurs	**Catastrophic** (death, loss of asset, mission capability or unit readiness)	I	1	1	1	2	3
	Critical (permanent disabling injury or damage, significantly degraded mission capability or unit readiness)	II	1	1	2	3	3
	Moderate (non-permanent disabling injury or damage, degraded mission capability or unit readiness)	III	2	2	3	4	4
	Negligible (minimal injury or damage, little or no impact to mission capability or unit readiness)	IV	3	3	4	4	4

Risk Assessment Codes (RAC)		
RAC Value	Risk Category	Action Required
1	Extremely High	stop, immediate correction
2	High	consider stopping, urgent correction
3	Moderate	corrective attention needed
4	Low	possible acceptance

Figure 24. Risk assessment matrix. Source: USCG Auxiliary, National Response Directorate

Figure 25 shows two of these axes in a two-dimensional chart. Once appropriate scenarios are devised and assigned a tier level (1-5), the scenario can be classified based upon its placement on the effort-reward chart. Scenarios in the high reward/low effort quadrant (upper right) are most likely the first where cyber defense resources should be directed whereas the low reward/high effort quadrant (lower left) are not areas of greatest vulnerability.

The simplicity of the two-dimensional risk models belies the complexity of the actual cybersecurity threats. Figure 26 shows all three axes of the Tam and Jones model in a three-dimension chart. In this particular case, the different technologies do not necessarily add to the difficulty of an attack, nor the potential reward for the attacker. Thus, it is the entire high reward/low effort plane that becomes the priority for cyber defense.

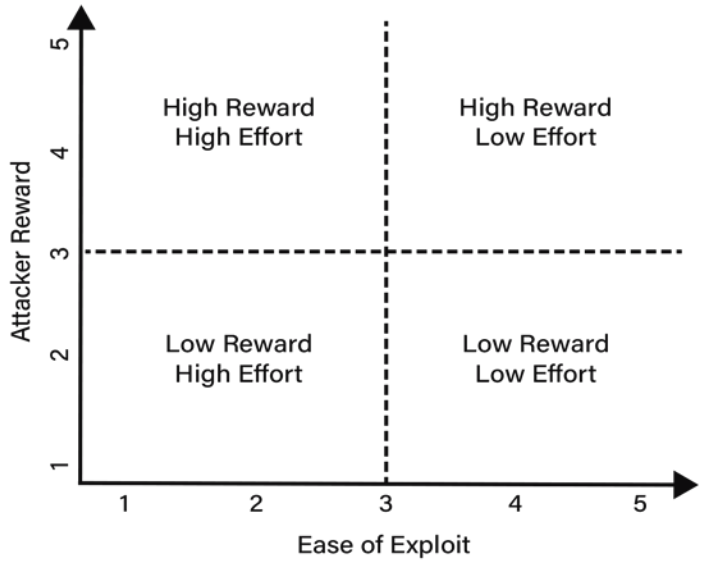


Figure 25. Two-dimension effort-reward chart. Source: Gary C. Kessler

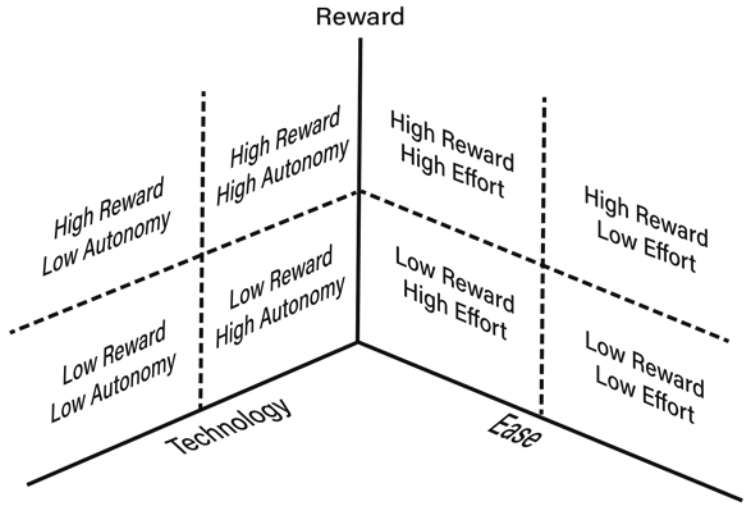


Figure 26. Three-dimension effort-reward-technology chart. Source: Gary C. Kessler

Acronyms

AAWA	Advanced Autonomous Waterborne Applications
AI	artificial intelligence
AIS	Automatic Identification System
AOA	angle of attack
APT	advanced persistent threat
ATON	aid to navigation
C4ADS	Center for Advanced Defense Studies
C/A	coarse/acquisition code
CAN	Controller Area Network
CDMA	code-division multiple access
CIA	Central Intelligence Agency
COSCO	China Ocean Shipping Company
COTS	commercial off-the-shelf
CPA	closest point of approach
CPS	cyber-physical systems
DCS	distributed control system
DHS	Department of Homeland Security
DDoS	distributed denial-of-service
DIB	defense industrial base
DNS	Domain Name System
DOD	U.S. Department of Defense
DoS	denial-of-service

ECDIS	electronic chart display and information system
EO	executive order
EU	European Union
EW	electronic warfare
FBI	Federal Bureau of Investigation
GLONASS	Global Navigation Satellite System (Russia)
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HMI	human-machine interface
ICS	industrial control systems
ICT	information and communications technology
IMU	inertial measurement units
IoT	Internet of Things
IP	internet protocol
ISS	International Space Station
IT	information technology
ITU	International Telecommunication Union
ITU-R	International Telecommunication Union, Radiocommunication Sector
IW	irregular warfare
LCS	littoral combat ships
LZ	littoral zone
MASS	maritime autonomous surface ships
MCAS	Maneuvering Characteristics Augmentation System
MEO	medium earth orbit

MHz	megahertz
ML	machine learning
MMSI	Maritime Mobile Service Identity
MSA	Maritime Safety Administration
MTS	Maritime Transportation System
NMEA	National Maritime Electronics Association
NSA	National Security Agency
OT	operational technology
P(Y)	precision code (encrypted)
PLA	People's Liberation Army
PLC	programmable logic controller
PNT	positioning, navigation, and timing
PPS	Precise Positioning Service
PRN	pseudorandom noise
RAT	remote access Trojan
RTU	remote terminal unit
SA	selective availability
SAR	search and rescue
SATCOM	satellite communications
SCADA	supervisory control and data acquisition
SDR	software-defined radio
SOF	Special Operations Forces
SOLAS	Safety of Life at Sea Convention
SPS	Standard Positioning Service

SVAN	Safer Vessel with Autonomous Navigation
Tbps	terabits per second
TTP	tactics, techniques, and procedures
UAV	unmanned aerial vehicle
UHF	ultra high frequency
UK	United Kingdom
USB	Universal Serial Bus
USCG	United States Coast Guard
USSOCOM	United States Special Operations Command
USV	unmanned surface vessel
UT	The University of Texas at Austin
UTC	Coordinated Universal Time

Endnotes

1. "A Ship in Harbor Is Safe, But that Is Not What Ships Are Built For: John A. Shedd? Grace Hopper? Albert Einstein? Anonymous?," Quote Investigator, 9 December 2013, https://quoteinvestigator.com/2013/12/09/safe-harbor/.
2. Joint Special Operations University, *Special Operations Research Topics 2020* (Tampa, FL: JSOU Press, 2019), https://jsou.libguides.com/ld.php?content_id=48680282.
3. U.S. Department of Defense, *Cyberspace Operations* Joint Publication 3-12 (R) (5 February 2013): v, https://fas.org/irp/doddir/dod/jp3_12r.pdf.
4. Norman Cigar, *The Jihadist Maritime Strategy: Waging a Guerilla War at Sea*, MES Monographs No. 8, Middle East Studies at the Marine Corps University (May 2017): https://www.usmcu.edu/Portals/218/MES/Monographs/MESM_8_MAY_2017_lo.pdf?ver=2018-10-16-110147-393.
5. Gary C. Kessler, "Cybersecurity in the Maritime Domain," *Proceedings of the USCG Marine Safety & Security Council* 76, no. 1 (Spring 2019): 34–39, https://www.dco.uscg.mil/Portals/9/DCO%20Documents/Proceedings%20Magazine/Archive/2019/Vol76_No1_Spring2019.pdf.
6. Chris Bing, "Chinese Hacking Group Resurfaces to Spy on U.S. Maritime Firms," *cyberscoop*, 16 March 2018, https://www.cyberscoop.com/chinese-hacking-group-south-china-sea/; Federal Bureau of Investigation (FBI), "APT 10 Group," *Most Wanted*, https://www.fbi.gov/wanted/cyber/apt-10-group.
7. Secretary of the Navy, "Cybersecurity and Readiness Review," March 2019, https://www.navy.mil/strategic/CyberSecurityReview.pdf.
8. Jahshan Bhatti and Todd E. Humphreys, "Hostile Control of Ships via False GPS Signals: Demonstration and Detection," *NAVIGATION: Journal of the Institute of Navigation* 64, no. 1 (Spring 2017), 51–66, https://onlinelibrary.wiley.com/doi/abs/10.1002/navi.183; Goward, "GNSS Spoofing"; Dana Goward, "How to Steal a Ship," *The Maritime Executive* (2 June 2017), https://maritime-executive.com/editorials/how-to-steal-a-ship.
9. Torbjorn Grimeland and Oscar van der Veen, "Maritime SOF in the Littorals: Theoretical Principles for Successful Littoral Special Operations" (thesis, Naval Postgraduate School, June 2016), https://core.ac.uk/download/pdf/45464821.pdf; Milan Vego, "On Littoral Warfare," *Naval War College Review* 68, no. 2, article 4 (Spring 2015): 2–3, https://digital-commons.usnwc.edu/nwc-review/vol68/iss2/4/; Paul Webb, *Introduction to Oceanography* (1 July 2019), https://rwu.pressbooks.pub/webboceanography/.
10. DOD, *DOD Dictionary of Military and Associated Terms* (November 2019): 132, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.
11. Robert H. Stewart, *Introduction to Physical Oceanography* (13 August 2008), https://open.umn.edu/opentextbooks/textbooks/20; Paul Webb, *Introduction*

to Oceanography, 1 July 2019, https://rwu.pressbooks.pub/webboceanography/; Jonathan White, *TIDES: The Science and Spirit of the Ocean* (San Antonio, TX: Trinity University Press, 2017).

12. William A. Berkemeier, Charles E. Long, and Kent K. Hathaway, "DELILAH, DUCK94 & SandyDuck: Three Nearshore Field Experiments," in *Proceedings of the 25th Conference on Coastal Engineering*, Orlando, Florida, 1996, https://icce-ojs-tamu.tdl.org/icce/index.php/icce/article/view/5529/5203; U.S. Army Corp of Engineers, "SandyDuck '97 Coastal Field Experiment," Field Research Facility, Coastal & Hydraulics Laboratory, 13 October 2004, http://www.frf.usace.army.mil/SandyDuck/SandyDuck.stm.
13. U.S. Energy Information Administration, "The Strait of Hormuz is the world's most important oil transit checkpoint," 20 June 2019, https://www.eia.gov/todayinenergy/detail.php?id=39932.
14. Vego, "On Littoral Warfare."
15. United Nations, "The Ocean Conference Fact Sheet," June 2017, https://www.un.org/sustainabledevelopment/wp-content/uploads/2017/05/Ocean-fact-sheet-package.pdf; U.S. Marine Corps, *Expeditionary Operations*, Marine Corps Doctrinal Publication (MCDP) 3 (Department of the Navy, 16 April 1998), https://www.marines.mil/Portals/1/Publications/MCDP%203.pdf.
16. Because the Moon has the largest daily gravitational effect on the tides, the tidal cycle on Earth is based upon a lunar day, which is approximately 24 hours and 50 minutes. The most common daily tidal pattern is *semi-diurnal*, with two high tides of roughly equal height and two low tides of roughly equal height. In some areas, one of the high (or low) tides might be more extreme than the other; this is called a *mixed* tidal cycle. In areas with a *diurnal* tide cycle, there is a single high and single low tide each day.
17. White, *TIDES*.
18. Keller, 2016; "Littoral Combat Ship Class—LCS," U.S. Navy Fact File, 20 December 2019, https://www.navy.mil/navydata/fact_display.asp?cid=4200&tid=1650&ct=4.
19. "Product Lines at SUPSHIP Bath," NAVSEA Supervisor of Shipbuilding, Conversion & Repair, 1 March 2012, https://web.archive.org/web/20120301113457/http://www.navsea.navy.mil/supship/Bath/Products.aspx.
20. Mark Gunzinger, Bryan Clark, David Johnson, and Jesse Sloman, "Force Planning for the Era of Great Power Competition," *Center for Strategic and Budgetary Assessments*, 2017, https://csbaonline.org/uploads/documents/CSBA6302_(Developing_the_Future_Force)_PRINT.pdf.
21. David Axe, "Israeli Navy Revamps for Hybrid, Littoral and Strategic Warfare," *Offiziere.ch*, 8 January 2010, https://www.offiziere.ch/?p=2507; John Keller, "Navy Looks to Modified Littoral Combat Ship as Next-Generation Frigate," *Military & Aerospace Electronics*, 19 April 2016, https://www.militaryaerospace.com/communications/article/16709025/navy-looks-to-modified-littoral-combat-ship-as-nextgeneration-frigate; "Navy looks to modified littoral combat ship design to serve as next-generation frigate," *Military &*

Aerospace Electronics, 15 March 2016, https://www.militaryaerospace.com/computers/article/16714504/navy-looks-to-modified-littoral-combat-ship-design-to-serve-as-nextgeneration-frigate.

22. Thomas Szayna, et. al. "Conflict Trends and Conflict Drivers: An Empirical Assessment of Historical Conflict Patterns and Future Conflict Projections," *RAND* Research Report (2017): 225, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1063/RAND_RR1063.pdf.
23. Opher Doran and David Eshel, "The Israelis Know Littoral Warfare," *Proceedings of the U.S. Naval Institute* 123, no. 3 (March 2003): 66; Joachim Kimpel, "Countering Asymmetric Threats in the Littoral Maritime Environment," Federal Office of Defense Technology and Procurement, Germany, 1 September 2006, https://apps.dtic.mil/dtic/tr/fulltext/u2/a485147.pdf.
24. Joseph DiRenzo III, Nicole K. Drumhiller, and Fred S. Roberts (Eds.), *Issues in Maritime Cyber Security* (Washington, D.C.: Westphalia Press, 2017); Kessler, "Cybersecurity in the Maritime Domain"; R. Sen, "Cyber and Information Threats to Seaports and Ships," in Michael A. McNicholas (Ed.), *Maritime Security: An Introduction*, 2nd. ed. (Amsterdam: Elsevier, 2016): 281–302.
25. Cigar, *Jihadist Maritime Strategy*.
26. Eric Schlosser, *Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety* (New York: The Penguin Press, 2013): 224, https://www.goodreads.com/quotes/tag/navigation.
27. Tristan Gooley, *How to Read Water: Clues and Patterns from Puddles to the Sea* (New York: The Experiment, 2016).
28. Laura Poppick, "The Story of the Astrolabe, the Original Smartphone," *Smithsonian Magazine*, 31 January 2017, https://www.smithsonianmag.com/innovation/astrolabe-original-smartphone-180961981/.
29. Pratap Misra and Per Enge, *Global Positioning System: Signals, Measurement, and Performance*, 2nd. edition (Lincoln, MA: Ganga-Jamuna Press, 2006).
30. Nathaniel Bowditch, *The American Practical Navigator: An Epitome of Navigation*, 2002 Bicentennial Edition (Bethesda, Maryland: National Imagery and Mapping Agency, 2002), https://www.nwcbooks.com/get/ebook.php ?id=hok-AAAAYAAJ; Misra and Enge, *Global Positioning System*.
31. Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, Tyler Way, and Makena Young, "Space Threat Assessment 2020," *Center For Strategic And International Studies (CSIS) Aerospace Security Project*, March 2020, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/200330_SpaceThreatAssessment20_WEB_FINAL1.pdf; DOD, 2013.
32. Eric Chabrow, "Aligning Electronic and Cyber Warfare: Similarities Exist Between the Two, but They Are Not the Same," *GovInfoSecurity*, 10 July 2012, https://www.govinfosecurity.com/aligning-electronic-cyber-warfare-a-4930; Sam Cohen, "Integrating Cyber and Electronic Warfare," *The CyberEdge*, 5 March 2018, https://www.afcea.org/content/integrating-cyber-and-electronic-warfare; Marc

Lichtman, Jeffrey D. Poston, SaiDhiraj Amuru, Chowdhury Shahriar, T. Charles Clancy, R. Michael Buehrer, and Jeffrey H. Reed, "A Communications Jamming Taxonomy," *IEEE Security & Privacy 14*, no. 1 (January/February 2016): 47–54, https://doi.org/10.1109/MSP.2016.13.

33. While this is a fine hair to split, the use of the term *assured PNT* rather than *secure GNSS* is very important, at least philosophically. The bottom line is that the military (and civilians) do not *need* a secure GNSS; they *need* assured PNT. While a secure GNSS would undoubtedly lead to assured PNT, one could argue that assured PNT in the absence of secure GNSS achieves the desired goal.
34. Kevin Coggins, "Assured PNT: A Path to Resilient Positioning, Navigation and Timing," *PM PNT Internal News and Announcements*, 6 February 2015, https://www.pmpnt.army.mil/assured-pnt/; Cole, "Securing Military GPS"; Dee Ann Divis, "DOD on Innovation Fast Track: Views of Top Pentagon PNT Managers," *Inside GNSS*, 20 December 2019, https://insidegnss.com/dod-on-innovation-fast-track-views-of-top-pentagon-pnt-managers/; DOD, *Dictionary of Military Terms*, 152.
35. Mike Sutton, "Special Operations Forces: Dual Redundancy for Denied Environments—From System to Soldier," https://www.orolia.com/sites/default/files/document-files/Special-Operations-Forces--Dual-Redundancy-for-GPS-GNSS-Denied-Environments-Final_0.pdf.
36. "Characterizing GNSS Interference from Low-Earth Orbit," *Inside GNSS*, 3 February 2020, https://insidegnss.com/characterizing-gnss-interference/.
37. Anton Lavrov, "Russia's GLONASS Satellite Constellation," *Centre for Analysis of Strategies and Technologies*, https://cast.ru/products/articles/russia-s-glonass-satellite-constellation.html.
38. NAVIC is the operational name for the Indian Regional Navigation Satellite System (IRNSS).
39. NovAtel Inc., *An Introduction to GNSS: GPS, GLONASS, BeiDou, Galileo and other Global Navigation Satellite Systems*, 2nd. ed., 2015, http://www2.novatel.com/GNSSBook.
40. K. Czaplewski and D. Goward, "Global Navigation Satellite Systems—Perspectives on Development and Threats to System Operation," *TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation* 10, no. 2 (June 2016): 183–192, https://doi.org/10.12716/1001.10.02.01.
41. Misra and Enge, *Global Positioning System*; DOD, "Global Positioning System Precise Positioning Service Performance Standard," February 2007, https://www.gps.gov/technical/ps/2007-PPS-performance-standard.pdf; DOD, "Global Positioning System Standard Positioning Service Performance Standard," 4th Edition, September 2008, http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf; Tyler Whiting, "GPS Celebrates 25th Year of Operation," 27 April 2020, https://www.spaceforce.mil/News/Article/2166101/gps-celebrates-25th-year-of-operation.
42. Global Positioning Systems (GPS) Directorate, "Systems Integration & Engineering Interface Specification," IS-GPS-200J, 25 April 2018, https://www.gps.gov/

technical/icwg/IS-GPS-200J.pdf; GPS.gov, "Space Segment," 26 November 2019, https://www.gps.gov/systems/gps/space/; Misra and Enge, *Global Positioning System*; NovAtel, *Introduction to GNSS*; DOD, "GPS Precise Positioning Service"; DOD, "GPS Standard Positioning Service."

43. Misra and Enge, *Global Positioning System*; NovAtel, *Introduction to GNSS*.
44. GPS.gov, "Space Segment"; Misra and Enge, *Global Positioning System*; NovAtel, *Introduction to GNSS*; DOD, "GPS Standard Positioning Service."
45. Jeff D. Coffed and Joe Rolli, "GPS & Shipping: Countering the Threat of Interference," in *Issues in Maritime Cyber Security*, ed. Joseph DiRenzo III, Nicole K. Drumhiller, and Fred S. Roberts (Washington, D.C.: Westphalia Press 2017): 397–405; Dana Goward, "GPS Jamming and Spoofing: Maritime's Biggest Cyber Threat," in *Issues in Maritime Cyber Security*, ed. DiRenzo III, Drumhiller, and Roberts, 407–415; NovAtel, *Introduction to GNSS*; Schweitzer Engineering Laboratories, "Mitigating GPS Vulnerabilities," 3 November 2014, https://selinc.com/solutions/synchrophasors/report/111935/.
46. Czaplewski and Goward, "Global Navigation Satellite Systems"; The Signal Jammer, 3 January 2020, https://www.thesignaljammer.com/categories/GPS-Jammers/.
47. Coffed and Rolli, "GPS & Shipping"; Goward, "GPS Jamming and Spoofing"; Kashmir Hill, "Jamming GPS Signals is Illegal, Dangerous, Cheap, and Easy," *Gizmodo*, 24 July 2017, https://gizmodo.com/jamming-gps-signals-is-illegal-dangerous-cheap-and-e-1796778955.
48. Alliance of Telecommunications Industry Solutions (ATIS), "GPS Vulnerability," ATIS Technical Report ATIS-0900005, 7 September 2017, https://access.atis.org/apps/group_public/download.php/36304/ATIS-0900005.pdf; Czaplewski and Goward, "Global Navigation Satellite Systems"; NovAtel, *Introduction to GNSS*.
49. Bit Banging Bytes, "Jamming Communications With SDR," 15 April 2018, https://bitbangingbytes.com/jamming-communications-with-sdr/; see also https://www.youtube.com/results?search_query=gps+jamming+with+sdr.
50. Charles Curry, "Detecting GPS Jammers: 'Gone in 20 Seconds,'" *CGSIC Annual Conference*, 8 September 2014, https://www.gps.gov/cgsic/meetings/2014/curry.pdf; Logan Scott, "J911: Fast Jammer Detection and Location Using Cell-Phone Crowd-Sourcings," *GPS World*, 1 November 2010, https://www.gpsworld.com/j911-fast-jammer-detection-10720/.
51. Matej Bažec, Blaž Luin, and Franc Dimc, "GPS Jamming Detection with SDR," ISEP 2016, *24th International Symposium on Electronics in Transport*, March 2016, https://www.researchgate.net/profile/Franc_Dimc/publication/304777109_GPS_Jamming_Detection_with_SDR/links/577a41a608ae213761c9ad4d/GPS-Jamming-Detection-with-SDR.pdf.
52. Dee Ann Divis, "Ship-Tracking Microsatellites Could Spot GPS Jammers From Space," *Inside GNSS*, 24 March 2020, https://rntfnd.org/2020/03/30/ship-tracking-microsatellites-could-spot-gps-jammers-from-space-inside-gnss/.

53. Coffed and Rolli, "GPS & Shipping"; Sally Cole, "Securing Military GPS From Spoofing and Jamming Vulnerabilities," *Military Embedded Systems*, n.d., http://mil-embedded.com/articles/securing-military-gps-spoofing-jamming-vulnerabilities/; Goward, "GPS Jamming and Spoofing"; NovAtel, *Introduction to GNSS*; Schweitzer Engineering Laboratories, "Mitigating GPS Vulnerabilities." GLONASS is also already available in many dual-constellation GNSS products but these are for civilian use. GLONASS has encrypted, high-precision signals for military use and unencrypted, standard-precision signals for civilian use.
54. ATIS, "GPS Vulnerability"; NovAtel, *Introduction to GNSS*; Schweitzer Engineering Laboratories, "Mitigating GPS Vulnerabilities."
55. Cole, "Securing Military GPS"; Czaplewski and Goward, "Global Navigation Satellite Systems."
56. ATIS, "GPS Vulnerability"; NovAtel, *Introduction to GNSS*; Schweitzer Engineering Laboratories, "Mitigating GPS Vulnerabilities"; Tech Minds, "GPS Spoofing With The HackRF on Windows," *Tech Minds* YouTube channel, 22 December 2019, https://www.youtube.com/watch?v=3NWn5cQM7q4.
57. Mark L. Psiaki and Todd E. Humphreys, "GPS Lies," *IEEE Spectrum 53*, issue 8, August 2016, 26–33.
58. Mark L. Psiaki and Todd E. Humphreys, "GNSS Spoofing and Detection," n.d., https://radionavlab.ae.utexas.edu/images/stories/files/papers/gnss_spoofing_detection.pdf; Psiaki and Humphreys, "GPS Lies."
59. Brady W. O'Hanlon, Mark L. Psiaki, Jahshan A. Bhatti, Daniel P. Shepard, and Todd E. Humphreys, "Real-Time GPS Spoofing Detection Via Correlation Of Encrypted Signals," *NAVIGATION: Journal Of The Institute Of Navigation 60*, issue 4 (Winter 2013): 267–278, https://doi.org/10.1002/navi.44; Mark L. Psiaki, Brady W. O'Hanlon, Jahshan A. Bhatti, Daniel P. Shepard, and Todd E. Humphreys, "GPS Spoofing Detection Via Dual-Receiver Correlation Of Military Signals," *IEEE Transactions on Aerospace and Electronic Systems 49*, issue 4 (October 2013): 2250–2267.
60. NovAtel, *Introduction to GNSS*; Schweitzer Engineering Laboratories, "Mitigating GPS Vulnerabilities."
61. ATIS, "GPS Vulnerability"; Alliance of Telecommunications Industry Solutions (ATIS), "GPS Vulnerability Report," 7 December 2016, https://www.gps.gov/governance/advisory/meetings/2016-12/calabro.pdf; Czaplewski and Goward, "Global Navigation Satellite Systems"; NTP Pool News, "GPS Rollover," 5 April 2019, https://news.ntppool.org/2019/04/gps-rollover/.
62. Misra and Enge, *Global Positioning System*.
63. Cole, "Securing Military GPS."
64. ATIS, "GPS Vulnerability"; ATIS, "GPS Vulnerability Report"; Schweitzer Engineering Laboratories, "Mitigating GPS Vulnerabilities."

65. Eric Gakstatter, "What Exactly is GPS NMEA Data?," *GPS World*, 4 February 2015, https://www.gpsworld.com/what-exactly-is-gps-nmea-data/; Lichtman et al., "Communications Jamming Taxonomy."
66. Ken Munro, "Crashing Ships by Hacking NMEA Sentences," Pen Test Partners, 26 March 2018, https://www.pentestpartners.com/security-blog/crashing-ships-by-hacking-nmea-sentences/.
67. Elisabeth Braw, "The GPS Wars Are Here," *Foreign Policy*, 17 December 2018, https://foreignpolicy.com/2018/12/17/the-gps-wars-are-here/, Mark Episkopos, "RIP GPS? Russia is Testing How it Can Jam NATO's Navigation Systems," *The National Interest*, 26 February 2020, https://nationalinterest.org/blog/buzz/rip-gps-russia-testing-how-it-can-jam-natos-navigation-systems-127142.
68. Goward, "GPS Jamming and Spoofing."
69. "FCC Fines Operator of GPS Jammer That Affected Newark Airport GBAS," *Inside GNSS*, 31 August 2013, https://insidegnss.com/fcc-fines-operator-of-gps-jammer-that-affected-newark-airport-gbas/; Chris Matyszczyk, "Truck Driver has GPS Jammer, Accidently Jams Newark Airport," *CNET*, 11 August 2013, https://www.cnet.com/news/truck-driver-has-gps-jammer-accidentally-jams-newark-airport/.
70. Bit Banging Bytes, "Jamming Communications"; Hill, "Jamming GPS Signals"; See https://www.jammer-store.com/, http://www.jammerfromchina.com/, and https://www.thesignaljammer.com/categories/GPS-Jammers/.
71. Resilient Navigation and Timing Foundation, "Prioritizing Dangers to the United States From Threats to GPS: Ranking Risks and Proposed Mitigations," White Paper, 30 November 2016, https://rntfnd.org/wp-content/uploads/12-7-Prioritizing-Dangers-to-US-fm-Threats-to-GPS-RNTFoundation.pdf.
72. "Spoofing a Superyacht at Sea," *UTNews,* 30 July 2013, https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea.
73. Psiaki and Humphreys, "GNSS Spoofing and Detection"; Psiaki and Humphreys, "GPS Lies."
74. Matt Burgess, "When a tanker vanishes, all the evidence points to Russia," *WIRED*, 21 September 2017, https://www.wired.co.uk/article/black-sea-ship-hacking-russia; Dana Goward, "Mass GPS Spoofing Attack in Black Sea?," *The Maritime Executive*, 11 July 2017, http://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea; Dana Goward, "GNSS Spoofing—A Technology Re/evolution," December 2018, https://www.gps.gov/governance/advisory/meetings/2018-12/goward.pdf; David Hambling, "Ships Fooled in GPS Spoofing Attack Suggest Russian Cyberweapon," *NewScientist*, 10 August 2017, https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/; U.S. Maritime Administration (MARAD), "Black Sea-GPS Interference," Maritime Security Communications with Industry (MSCI) Advisory 2017-005A (22 June 2017), https://www.maritime.dot.gov/content/2017-005a-black-sea-gps-interference.
75. Alan Cameron, "Russia Practices Widespread Spoofing," *GPS World*, 2 April 2019, https://www.gpsworld.com/russia-practices-widespread-spoofing; Center

for Advanced Defense Studies (C4ADS), "Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria," 2019, https://www.c4reports.org/aboveusonlystars; John E. Dunn, "Russia Accused of Massive GPS Spoofing Campaign," *Naked Security by Sophos*, 1 April 2019, https://nakedsecurity.sophos.com/2019/04/01/russia-accused-of-massive-gps-spoofing-campaign/; Harrison et al., "Space Threat Assessment 2020."

76. Katherine Dunn, "Insight: Cyber Threats to Shipping Grow in East Mediterranean," *S&P Global Platts*, 21 November 2018, https://blogs.platts.com/2018/11/21/insight-cyber-threats-shipping-east-mediterranean/; Judah Ari Gross, "GPS Jamming Affecting Israel Comes From Russian Base in Syria: US Researcher," *The Times of Israel*, 28 June 2019, https://www.timesofisrael.com/gps-jamming-affecting-israel-comes-from-russian-base-in-syria-us-researcher/; "Russia is Jamming GPS Systems of Powerful F-22 Raptors, F-35 Jets in Middle East," *The EurAsian Times*, 9 February 2020, https://eurasiantimes.com/russia-is-jamming-gps-systems-of-powerful-f-22-raptors-f-35-jets-in-middle-east.

77. MARAD, "Eastern Mediterranean Sea-GPS Interference," MSCI Advisory 2018-007, 7 May 2018, https://www.maritime.dot.gov/content/2018-007-eastern-mediterranean-sea-gps-interference; MARAD, "Eastern Mediterranean Sea-GPS Interference," MSCI Advisory 2018-014, 8 November 2018, https://www.maritime.dot.gov/content/2018-014-eastern-mediterranean-sea-gps-interference.

78. Katherine Dunn, "Mysterious GPS outages are wracking the shipping industry," *Fortune*, 22 January 2020, https://fortune.com/longform/gps-outages-maritime-shipping-industry/; Katherine Dunn, "The Long Ocean Voyage That Helped Find The Flaws in GPS," *Fortune*, 24 January 2020, https://fortune.com/2020/01/24/gps-disruption-test-voyage/; E. Pérez Marcos, Andriy Konovaltsev, Stefano Caizzone, Manuel Cuntz, Kazeem Yinusa, Wahid Elmarissi, and Michael Meurer, "Interference and Spoofing Detection for GNSS Maritime Applications using Direction of Arrival and Conformal Antenna Array," *31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018)*, (2018): 2907–2922, https://doi.org/10.33012/2018.15901.

79. C4ADS, "Above Us Only Stars"; Goward, "GNSS Spoofing"; "GPS Spoofing Patterns Discovered," *The Maritime Executive*, 27 September 2017, https://www.maritime-executive.com/article/gps-spoofing-patterns-discovered; Elizabeth Weise, "Mysterious GPS Glitch Telling Ships They're Parked at Airport May be Anti-Drone Measure," *USA TODAY*, 3 October 2017, https://www.usatoday.com/story/tech/news/2017/09/26/gps-spoofing-makes-ships-russian-waters-think-theyre-land/703476001/.

80. Michelle Wiese Bockmann, "Seized UK Tanker Likely 'Spoofed' by Iran," *Lloyd's List*, 16 August 2019, https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran; Barbara Starr, Ryan Browne, and Kara Fox, "Iran Announces Capture of British-Flagged Oil Tanker; U.S. Officials Say Two Ships Seized," 19 July 2019, https://www.cnn.com/2019/07/19/middleeast/british-tanker-seized-iran-intl/index.html.

81. Dana Goward, "GPS Jamming and Spoofing Reported at Port of Shanghai," *Maritime Executive*, 13 August 2019, https://www.maritime-executive.com/editorials/gps-jamming-and-spoofing-at-port-of-shanghai; also in *Resilient Navigation and Timing Foundation*, 13 August 2019, https://rntfnd.org/2019/08/14/gps-jamming-and-spoofing-reported-at-port-of-shanghai-maritime-executive/; Mark Harris, "Ghost Ships, Crop Circles, and Soft Gold: A GPS Mystery in Shanghai," *MIT Technology Review*, 15 November 2019, https://www.technologyreview.com/s/614689/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/; Joseph Trevithick, "New Type Of GPS Spoofing Attack In China Creates 'Crop Circles' Of False Location Data," *The War Zone Wire*, 18 November 2019, https://www.thedrive.com/the-war-zone/31092/new-type-of-gps-spoofing-attack-in-china-creates-crop-circles-of-false-location-data.
82. C4ADS, "Shanghai GPS Spoofing," 2 December 2019, https://drive.google.com/file/d/1dTWu7H9JjRyN0uQPZ9HwiUzCFd7cd5pL/view; Harris, "Ghost Ships"; Harrison et al., "Space Threat Assessment 2020"; Trevithink, "New Type Of GPS Spoofing."
83. Bjorn Bergman, "AIS Ship Tracking Data Shows False Vessel Tracks Circling Above Point Reyes, Near San Francisco," *Skytruth*, 26 May 2020, https://skytruth.org/blog/; Dana Goward, "GPS Circle Spoofing Discovered in Iran," *GPS World*, 21 April 2020, https://www.gpsworld.com/gps-circle-spoofing-discovered-in-iran/; Dana Goward, "New GPS 'Circle Spoofing' Moves Ship Locations Thousands of Miles," *GPS World*, 26 May 2020, https://www.gpsworld.com/new-gps-circle-spoofing-moves-ship-locations-thousands-of-miles/.
84. Mark Rockwell, "Executive Order Looks to Safeguard GPS Infrastructure," *FCW*, 12 February 2020, https://fcw.com/articles/2020/02/12/order-pmt-gps-rockwell.aspx. Interestingly, some think that the Executive Order will actually slow the design and implementation of solutions by delaying market-driven solutions; e.g., see Dana Goward, "PNT Executive Order Helpful, but Delays Market Solutions," *GPS World*, 20 February 2020, https://www.gpsworld.com/pnt-executive-order-needlessly-delays-market-driven-solutions/.
85. Dana Goward, "U.S. Coast Guard Protests GPS Disruption to UN Body: 'Urgent Issue'," *GPS World*, 26 March 2020, https://rntfnd.org/2020/03/26/us-coast-guard-protests-gps-disruption-to-un-body-urgent-issue-gps-world/.
86. United States Government Accountability Office (GAO), "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities," GAO-19-128, 9 October 2018, https://www.gao.gov/assets/700/694913.pdf.
87. Tackling GNSS Interference, *Global Military Communications*, 8, April 2018, http://www.satelliteevolutiongroup.com/articles/GNSS.pdf.
88. *Maritime Double Shots*, https://www.goodreads.com/quotes/tag/maritime.
89. Cigar, *Jihadist Maritime Strategy*.
90. Both IMO and USCG AIS requirements exempt warships.

91. "Navy Ships in Crowded Seas to Broadcast Locations," *Stars and Stripes*, 1 October 2017, https://www.military.com/daily-news/2017/10/01/navy-ships-in-crowded-seas-to-broadcast-locations.html.

92. International Maritime Organization (IMO), "Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS)," Resolution A.917(22), 25 January 2002, https://www.navcen.uscg.gov/pdf/AIS/IMO_A_917(22)_AIS_OPS_Guidelines.pdf.

93. Richard Gray, "The Hunt for Fish Pirates Who Exploit the Sea," *BBC Future*, 18 February 2019, https://www.bbc.com/future/article/20190213-the-dramatic-hunt-for-the-fish-pirates-exploiting-our-seas; Harris, "Ghost Ships"; Chris Lo, "GPS Spoofing: What's the Risk for Ship Navigation," *Ship Technology*, 15 April 2019, https://www.ship-technology.com/features/ship-navigation-risks/; Nicholas Newman, "Cyber Pirates Terrorising the High Seas," *Engineering and Technology*, 18 April 2019, https://eandt.theiet.org/content/articles/2019/04/cyber-pirates-terrorising-the-high-seas/; Andrew Palmer, *The New Pirates: Modern Global Piracy from Somalia to the South China Sea* (London: I.B. Tauris, 2014).

94. NMEA, "OneNet Standard for IP Networking of Marine Electronic Devices," 2019, https://www.nmea.org/content/STANDARDS/OneNet.

95. Marco Balduzzi, Alessandro Pasta, and Kyle Wilhoit, "A Security Evaluation of AIS Automated Identification System," in *Proceeding the 30th Annual Computer Security Applications Conference* (ACSAC '14), New Orleans, Louisiana, 8–12 December 2014, 436–445, ; Marco Balduzzi, Kyle Wilhoit, and Alessandro Pasta, "A Security Evaluation of AIS," Trend Micro Research Paper, December 2014, https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf.

96. Athanassios Goudossis and Sokratis K. Katsikas, "Towards a secure automatic identification system (AIS)," *Journal of Marine Science and Technology, 24*(2), June 2019, 410–423, DOI: 10.1007/s00773-018-0561-3.

97. Gary C. Kessler, John P. Craiger, and Jon Haass, "A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System," *TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation* 12, no. 3 (September 2018): 429–437, https://doi.org/10.12716/1001.12.03.01.

98. Balduzzi et al., "Security Evaluation of AIS"; Balduzzi et al., "Security Evaluation of Automated Identification System"; Firstpost, "Trend Micro Warns of Vulnerabilities in Global Vessel Tracking Systems," 3 February 2017, https://www.firstpost.com/business/biztech/business-tech/security/trend-micro-warns-of-vulnerabilities-in-global-vessel-tracking-systems-1895547.html.

99. Gary C. Kessler, "AIS Research Using a Raspberry Pi," 16 May 2020, https://www.garykessler.net/library/ais_pi.html; RTL-SDR.COM, "Using the RTL-SDR as a Transmitter," 21 June 2015, https://www.rtl-sdr.com/using-the-rtl-sdr-as-a-transmitter/; RTL-SDR.COM, "Setting Up a Raspberry Pi

Based Receiver With an RTL-SDR," 7 April 2016, https://www.rtl-sdr.com/setting-up-a-raspberry-pi-based-ais-receiver-with-an-rtl-sdr/.

100. AIS BlackToolkit, https://github.com/trendmicro/ais; Gary Kessler's AIS Tools, https://www.garykessler.net/software/index.html#ais; Gary C. Kessler, "Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity," *TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation 14*, no. 2 (June 2020), https://www.transnav.eu/Journal_Vol._14_No._2-June_2020,54.html.
101. https://opencpn.org/.
102. Kessler, "Protected AIS."
103. Kessler, "Protected AIS."
104. Harris, "Ghost Ships."
105. Bergman, "AIS Ship Tracking"; Goward, "New GPS 'Circle Spoofing.'"
106. https://www.goodreads.com/quotes/tag/malware.
107. John Costello, "China's Irregular Warfare in the Cyber Domain," *Real Clear Defense*, https://www.realcleardefense.com/articles/2015/06/18/chinas_irregular_warfare_in_the_cyber_domain_108094.html.
108. Brian Krebs, "WikiLeaks Dumps Docs on CIA's Hacking Tools," *Krebs on Security*, 8 March 2017, https://krebsonsecurity.com/2017/03/wikileaks-dumps-docs-on-cias-hacking-tools/; Panda Security, "Not Just WannaCry: The EternalBlue Exploit Gives Rise to More Attacks," *PandaLabs*, 18 May 2017, https://www.pandasecurity.com/mediacenter/pandalabs/wannacry-eternalblue-exploit-more-attacks/; Andy Greenberg, *SANDWORM* (New York: Doubleday, 2019).
109. The SMB service provides file, printer, device, and other forms of resource sharing for Windows networks.
110. Microsoft, "Microsoft Security Bulletin MS17-010—Critical: Security Update for Microsoft Windows SMB Server (4013389)," 14 March 2017, https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010; Microsoft, "Trojan:Win32/EternalBlue," *Microsoft Security Intelligence*, 3 August 2018, https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/EternalBlue&ThreatID=-2147239042.
111. The official end-of-life for Windows XP was 8 April 2014; see Microsoft, "Support for Windows XP Ended," n.d., https://www.microsoft.com/en-us/microsoft-365/windows/end-of-windows-xp-support.
112. Matthew Field, "WannaCry Cyber Attack Cost the NHS £92M as 19,000 Appointments Cancelled," *The Telegraph*, 11 October 2018, https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/; Agamoni Ghosh, "WannaCry: List of Major Companies and Networks Hit by Ransomware Around the Globe," 16 May 2017, https://www.ibtimes.co.uk/wannacry-list-major-companies-networks-hit-by-deadly-ransomware-around-globe-1621587; Greenberg, *SANDWORM*.

113. MalwareTech, "How to Accidently Stop a Global Cyber Attacks," MalwareTech Blog, 13 May 2017, https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html; Microsoft Security Response Center, "Customer Guidance for WannaCry Attacks," 12 May 2017, https://msrc-blog.microsoft.com/2017/05/12/customer-guidance-for-wannacrypt-attacks/; Iain Thomson, "While Microsoft Griped About NSA Exploit Stockpiles, it Stockpiled Patches: Friday's WinXP Fix Was Built in February," *The Register*, 16 May 2017, https://www.theregister.co.uk/2017/05/16/microsoft_stockpiling_flaws _too; Tom Warren, "Microsoft Issues 'Highly Unusual' Windows XP Patch to Prevent Massive Ransomware Attack," *The Verge*, 31 May 2017, https://www.theverge.com/2017/5/13/15635006/microsoft-windows-xp-security-patch-wannacry-ransomware-attack.
114. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *WIRED*, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; Greenberg, *SANDWORM*; Brian Krebs, "'Petya' Ransomware Outbreak Goes Global," *Krebs on Security*, 27 June 2017, https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/; Doug Olenick, "NotPetya Attack Totally Destroyed Maersk's Computer Network: Chairman," *SC Magazine*, 26 January 2018, https://www.scmagazine.com/notpetya-attack-totally-destroyed-maersks-computer-network-chairman/article/739730/; Danny Palmer, "Petya Ransomware: Cyberattack Costs Cold Hit $200M for Shipping Giant Maersk," *ZDNet*, 16 August 2017, http://www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/.
115. Olenick, "NotPetya Attack."
116. Robert Abel, "Ransomware Attack Knock Out Shipping Giant COSCO's U.S. Network," *SC Magazine*, 26 July 2018, https://www.scmagazine.com/home/security-news/cybercrime/ransomware-attack-knocks-out-shipping-giant-coscos-u-s-network/; Mark Edward Nero, "Long Beach Port Terminal Hit by Ransomware Attack," *Press-Telegram*, 24 July 2018, https://www.presstelegram.com/2018/07/24/long-beach-port-terminal-hit-by-ransomware-attack/; Pierluigi Paganini, "Ransomware Attack Against COSCO Spread Beyond its U.S. Networks to Americas," *Security Affairs*, 31 July 2018, https://securityaffairs.co/wordpress/74941/malware/cosco-ransomware-attack-followup.html.
117. Catalin Cimpanu, "Port of San Diego Suffers Cyber-Attack, Second Port in a Week After Barcelona," *ZDNet*, 27 September 2018, https://www.zdnet.com/article/port-of-san-diego-suffers-cyber-attack-second-port-in-a-week-after-barcelona/; Ionut Ilascu, "Port of Barcelona Suffers Cyberattack," *BleepingComputer*, 21 September 2018, https://www.bleepingcomputer.com/news/security/port-of-barcelona-suffers-cyberattack/; "Port of San Diego Hit by Cyberattack," *The Maritime Executive*, 27 September 2018, https://maritime-executive.com/article/port-of-san-diego-hit-by-cyberattack.
118. Catalin Cimpanu, "US Coast Guard Discloses Ryuk Ransomware Infection at Maritime Facility," *ZDNet*, 30 December 2019, https://www.zdnet.com/article/

us-coast-guard-discloses-ryuk-ransomware-infection-at-maritime-facility/; U.S. Coast Guard, "Cyberattack Impacts MTSA Facility Operations," *Marine Safety Information Bulletin (MSIB) Number 10-19* (16 December 2019), https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf.

119. Eduard Kovacs, "Australian Shipping Giant Toll Hit by Ransomware for Second Time," *SecurityWeek*, 6 May 2020, https://www.securityweek.com/australian-shipping-giant-toll-hit-ransomware-second-time; Martyn Wingrove, "Toll Suffers Second Cyber attack in Four Months," *Riviera*, 7 May 2020, https://www.rivieramm.com/news-content-hub/news-content-hub/toll-suffers-second-cyber-attack-in-four-months-59287.

120. BIMCO, "The Guidelines on Cyber Security Onboard Ships," Version 3, 2018, https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/cyber-security-guidelines-2018.ashx; Catalin Cimpanu, "Ships Infected With Ransomware, USB Malware, Worms," *ZDNet*, 12 December 2018, https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms/; "Tests Show Ease of Hacking ECDIS, Radar and Machinery," *The Maritime Executive*, 21 December 2017, https://maritime-executive.com/article/tests-show-ease-of-hacking-ecdis-radar-and-machinery; Vincent Wee, "Naval Dome Exposes Vessel Vulnerabilities to Cyber Attack," *Seatrade Maritime News*, 22 December 2017, https://www.seatrade-maritime.com/asia/naval-dome-exposes-vessel-vulnerabilities-cyber-attack.

121. Jon Boyens, Celia Paulsen, Rama Moorthy, and Nadya Bartol, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," *National Institute for Standards and Technology (NIST) Special Publication 800-161* (April 2015), http://dx.doi.org/10.6028/NIST.SP.800-161.

122. Paul Barnes and Richard Oloruntoba, "Assurance of Security in Maritime Supply Chains: Conceptual Issues of Vulnerability and Crisis Management," *Journal of International Management 11* (2005): 519–540; Boyens et al., "Supply Chain Risk Management"; Honglu Liu, Zhihong Tian, Anqiang Huang, and Zaili Yang, "Analysis of Vulnerabilities in Maritime Supply Chains," *Reliability Engineering & System Safety 169* (January 2018): 475–484, https://doi.org/10.1016/j.ress.2017.09.018.

123. CyberKeel, "Maritime Cyber-Risks," 15 October 2014, https://www.sfmx.org/wp-content/uploads/2017/03/Maritime-Cyber-Crime-10-2014.pdf; TrapX Research Labs, "Anatomy of an Attack: Zombie Zero—Weaponized Malware Targets ERP Systems," *TrapX Security*, 1 March 2017, http://www.trapx.com/wp-content/uploads/2014/07/TrapX_ZOMBIE_Report_Final.pdf.

124. Boyens et al., "Supply Chain Risk Management"; CyberKeel, "Maritime Cyber-Risks."

125. Catalin Cimpanu, "Popular Android Keyboard App Caught Collecting User Data, Running External Code," *Bleeping Computer*, 23 September 2017, https://www.bleepingcomputer.com/news/security/popular-android-keyboard-app-caught-collecting-user-data-running-external-code/; Swati Khandelwal, "Built-in

Keylogger Found in MantisTek GK2 Keyboards—Sends Data to China," *The Hacker News*, 7 November 2017, https://thehackernews.com/2017/11/mantistek-keyboard-keylogger.html.

126. Boyens et al., "Supply Chain Risk Management"; Paolo Zialcita, "U.S. Company Accused of Illegally Selling Chinese-Made Security Products to Military," *NPR*, 7 Nov 2019, https://www.npr.org/2019/11/07/777374783/u-s-company-accused-of-illegally-selling-chinese-made-security-products-to-milit.

127. Michele Acciaro and Patrizia Serra, "Maritime Supply Chain Security: A Critical Review," in *International Forum on Shipping, Ports and Airports (IFSPA) 2013: Trade, Supply Chain Activities and Transport: Contemporary Logistics and Maritime Issues* (3–5 June 2013): 636–651, https://www.researchgate.net/publication/275247061; Boyens et al., "Supply Chain Risk Management"; Defense Logistics Agency (DLA), "Supply Chain Security Strategy: Strengthening Operational Resiliency, Appendix 1 to DLA's 2018–2026 Strategic Plan," June 2019, https://www.dla.mil/Portals/104/Documents/Headquarters/StrategicPlan/SupplyChainSecurityStrategy.pdf; Saeyeon Roh, Jason Tam, Sung-Woo Lee, and Young-Joon Seo, "Risk assessment of maritime supply chain security in ports and waterways," *International Journal of Supply Chain. Management 7*, No. 6 (December 2018): 300–307, https://core.ac.uk/reader/195285825; Vijay Sakhuja, "Security Threats and Challenges to Maritime Supply Chains," 2010, *United Nations Institute for Disarmament Research*, https://www.peacepalacelibrary.nl/ebooks/files/UNIDIR_pdf-art2959.pdf.

128. Hausi A. Müller, "The Rise of Intelligent Cyber-Physical Systems," *IEEE Computer Magazine* 50, no. 12 (December 2017): 7–9.

129. Müller, "The Rise of Intelligent"; Dimitrios Serpanos, "The Cyber-Physical Systems Revolution," *IEEE Computer Magazine* 51, no. 3 (March 2018): 70–73.

130. Christof Ebert and Alpana Dubey, "Convergence of Enterprise IT and Embedded Systems," *IEEE Software* 36, no. 3 (May/June, 2019): 92–97; Dave Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," *Cisco Systems White Paper*, April 2011, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf; National Institute for Standards and Technology (NIST), "Framework for Cyber-Physical Systems: Volume 1, Overview," Version 1.0, Cyber-Physical Systems Public Working Group, Smart Grid and Cyber-Physical Systems Program Office Engineering Laboratory, *NIST Special Publication 1500-201*, June 2017, https://doi.org/10.6028/NIST.SP.1500-201; Mark Weiser, "The Computer for the 21st Century," *Scientific American* 265, no. 3 (March 1991): 94–104; Feng Xia, Laurence T. Yang, Lizhe Wang, and Alexey Vinel, "Internet of Things," International Journal of Communication Systems 25 (2012): 1101–1102; Li Da Xu, Wu He, and Shancang Li, "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics* 10, no. 4 (November 2014): 2233–2243.

131. Statista Research Department, "Internet of Things—Number of Connected Devices Worldwide, 2015–2025," *Statista*, 14 November 2019, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

132. Padraig Scully, "The Top 10 IoT Segments in 2018—Based on 1,600 Real IoT Projects," *IoT Analytics*, 2018, https://iot-analytics.com/top-10-iot-segments-2018-real-iot-projects/; Felix Wortmann and Kristina Flüchter, "Internet of Things," *Business & Information Systems Engineering* 57, no. 3 (June 2015): 221–224.
133. Lisa Kaiser, "Transportation Industrial Control Systems (ICS) Cybersecurity Standards Strategy," *U.S. Department of Homeland Security*, 7 December 2012, https://www.hsdl.org/?view&did=797578; U.S. Department of Homeland Security, "Roadmap to Secure Control Systems in the Transportation Sector," *The Roadmap to Secure Control Systems in the Transportation Sector Working Group*, August 2012, https://ics-cert.us-cert.gov/sites/default/files/documents/Transportation-Roadmap20120831.pdf.
134. Klaas van Dokkum, *Ship Knowledge: Ship Design, Construction and Operation*, 9th ed. (Vlissingen, The Netherlands: Dokmar Maritime Publishers BV, 2016).
135. Offshore Engineering, "Introduction to Dynamic Positioning," n.d., https://offshoreengineering.com/education/dynamic-positioning-dp/what-is-dynamic-positioning; van Dokkum, 2016.
136. "Ship Automation & Control System," *shippipedia*, n.d., http://www.shippipedia.com/ship-automation-control-system/; van Dokkum, 2016.
137. Wilhelmsen, "Intelligent Mooring with Timm Smart Ropes," n.d., https://www.wilhelmsen.com/marine-products/ropes/intelligent-mooring-with-timm-smart-ropes/.
138. Zebo Feng, Xiaoping Wu, Liangli Ma, and Wei Ren, "Toward Cyber-Physical Networks and Smartly Active Sensing IETM for Equipment Maintenance in Marine Ships," in *Proceedings of IET International Conference on Information and Communications Technologies (IETICT 2013)*: 599–603.
139. M. Matczak, "Intelligent container terminals—ITS solutions for seaports," *Archives of Transport System Telematics* 6, no. 2 (2013): 35–40; U.S. Department of Homeland Security, *Emerging Systems at Automated Container Terminals*, Operational Analysis Division, National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis (OCIA), 14 September 2017; Tingting Yang, Hailong Feng, Chengming Yang, Zhonghua Sun, Jiadong Yang, Fan Sun, Ruilong Deng, and Zhou Su, "Cooperative Networking towards Maritime Cyber Physical Systems," *International Journal of Distributed Sensor Networks* 2016, article id 3906549 (2016), https://doi.org/10.1155/2016/3906549.
140. Sheraz Aslam, Michalis P. Michaelides, and Herodotos Herodotou, "Internet of Ships: A Survey on Architectures, Emerging Applications, and Challenges," *IEEE Internet of Things Journal* (8 May 2020), https://doi.org/10.1109/JIOT.2020.2993411; Ivica Kuzmanić, Zlatan Kulenović, and Igor Vujović, "Contribution to Cross-Platform Programming in Integrated Ship's Systems," in Proceedings of 20th International Research/Expert Conference, Trends in the Development of Machinery and Associated Technology (TMT 2016), 24 September–1 October, 2016, 269–272.

141. Luca Urciuoli, "An Algorithm for Improved ETAs Estimations and Potential Impacts on Supply Chain Decision Making," *Procedia Manufacturing* 25 (2018): 185–193, https://doi.org/10.1016/j.promfg.2018.06.073.
142. Auto-Maskin, "DCU 210E Engine Controller," https://www.auto-maskin.com/prod/dcu-210e; Auto-Maskin, "Marine Pro Observer," https://apps.apple.com/cz/app/marine-pro-observer/id1462043697; Auto-Maskin, "Marine Pro Observer," https://www.similarplay.com/automaskin/marine_pro_observer/apps/se.automaskin; Auto-Maskin, "RP 210E Remote Panel," https://www.auto-maskin.com/prod/rp-210e.
143. CERT Coordination Center (CERT/CC), "Auto-Maskin DCU 210E RP 210E and Marine Pro Observer App," Vulnerability Note VU#176301, *Carnegie Mellon University, Software Engineering Institute*, 16 October 2018, https://www.kb.cert.org/vuls/id/176301/.
144. National Institute of Standards and Technology (NIST), "CVE-2017-6343-Detail," *National Vulnerability Database*, 2 October 2019, https://nvd.nist.gov/vuln/detail/CVE-2017-6343; "Vessel Video Camera Hack Update," Tactical Cyber Intelligence Report TR-130-2017, *The Maritime & Port Security Information Sharing & Analysis Organization (MPS-ISAO)*, 29 September 2017.
145. National Institute of Standards and Technology (NIST), "CVE-2013-6117-Detail," *National Vulnerability Database*, 14 July 2014, https://nvd.nist.gov/vuln/detail/CVE-2013-6117; "Vessel Video Camera Hack."
146. Metadata is system- or application-inserted data that describes characteristics about a file's contents. In a photograph taken via a digital camera on the Internet, metadata might include such information as the date and time that the photo was taken, camera type, camera settings, IP address, and latitude and longitude.
147. "Social Media Claim—Vessel Camera Hack," Warning Report WR-18-10-07, *The Maritime & Port Security Information Sharing & Analysis Organization (MPS-ISAO)*, 12 October 2018.
148. Cobham, "Sailor 900 VSAT," https://www.cobham.com/communications-and-connectivity/satcom/satellite-communication-at-sea/ku-band-maritime-vsat/sailor-900-vsat/.
149. US-CERT, "Cobham Sailor 900 VSAT Buffer Overflow Vulnerability," ICS Alert (ICS-ALERT-15-030-01), *Cybersecurity & Infrastructure Security Agency (CISA), U.S. Department of Homeland Security*, 30 January 2015, https://www.us-cert.gov/ics/alerts/ICS-ALERT-15-030-01.
150. Ken Munro, "OSINT From Ship Satcoms," *Pen Test Partners*, 13 October 2017, https://www.pentestpartners.com/security-blog/osint-from-ship-satcoms/; Ken Munro, "Tracking & Hacking Ships With Shodan & AIS," *Pen Test Partners*, 3 January 2018, https://www.pentestpartners.com/security-blog/tracking-hacking-ships-with-shodan-ais/; Ken Munro, "Satellite Communications Equipment Security," *Pen Test Partners*, 13 December 2018, https://www.pentestpartners.com/security-blog/satellite-communications-equipment-security/.

151. Ruben Santamarta, "A Wake-up Call for SATCOM Security," *IOActive Technical White Paper*, 2014, https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf; Ruben Santamarta, "Last Call for Satcom Security," *Black Hat 2018*, August 2018, http://i.blackhat.com/us-18/Thu-August-9/us-18-Santamarta-Last-Call-For-Satcom-Security.pdf; Ruben Santamarta, "Last Call for SATCOM Security," *IOActive White Paper*, August 2018, http://i.blackhat.com/us-18/Thu-August-9/us-18-Santamarta-Last-Call-For-Satcom-Security-wp.pdf.
152. Fantasia & Fiesta, "Forgotten Sister: The Zenobia Story," *HHV Ferry*, n.d., http://www.hhvferry.com/zenobia.html; Alan P. Newman, "The Zenobia Shipwreck," *Atlas Obscura*, n.d., https://www.atlasobscura.com/places/the-zenobia-shipwreck-larnaca-cyprus; B. N. Sullivan, "Diving the Wreck of the Zenobia—Introduction," *The Right Blue*, April 2008, https://therightblue.blogspot.com/2008/04/diving-wreck-of-zenobia-introduction.html; B. N. Sullivan, "The Wreck of the Zenobia—A Brief History," *The Right Blue*, April 2008, https://therightblue.blogspot.com/2008/04/wreck-of-zenobia-brief-history.html.
153. Paul Clifton, "Hoegh Osaka Ship was 'Unstable' When it Left Southampton Port," *BBC News*, 17 March 2016, https://www.bbc.com/news/uk-england-hampshire-35823182.
154. John Bacon, "Four Missing After Ship Capsizes, Burns Near Georgia Coast," *USA Today*, 8 September 2019, https://www.usatoday.com/story/news/nation/2019/09/08/four-missing-after-ship-capsizes-burns-near-georgia-coast/2255568001/; Gordon Jackson, "Pilot Praised for Decision to Ground Golden Ray," *The Brunswick News*, 3 October 2019, https://thebrunswicknews.com/news/local_news/pilot-praised-for-decision-to-ground-golden-ray/article_9bb34ae1-eae5-5dd4-a08d-6feeccc1d05b.html.
155. Jennifer Daffron, Simon Ruffle, Andrew Coburn, Jennifer Copic, Kelly Quantrill, Kayla Strong, and Eireann Leverett, "Shen Attack: Cyber Risk in Asian Ports," *Cambridge Centre for Risk Studies*, October 2019, https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2019/shen-attack/cyrim_shenattack_finalreport.pdf; Leonard Heilig, Eduardo Lalla-Ruiz, and Stefan Voß, "Digital transformation in maritime ports: analysis and a game theoretic framework," *NETNOMICS: Economic Research and Electronic Networking* 18, (2017): 227–254, https://link.springer.com/content/pdf/10.1007/s11066-017-9122-x.pdf; Leonard Heilig, Silvia Schwarze, and Stefan Voß, "An Analysis of Digital Transformation in the History and Future of Modern Ports," in *Proceedings of the 50th Hawaii International Conference on System Sciences* (January 2017): 1341–1350, https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1198&context=hicss-50; A. Karaś, "Smart Port as a Key to the Future Development of Modern Ports," *TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation* 14, no.1 (March 2020): 27–31, http://doi.org/10.12716/1001.14.01.01; Anahita Molavi, Gino J. Lim, Bruce Race, and Jian Shi, "Smart Ports: The Future of Maritime Transportation," in *Proceedings of THC-IT-2019 Conference & Exhibition*, 2019, http://hurricane.egr.uh.edu/sites/hurricane.egr.uh.edu/files/files/2019/SMART-PORTS-THE-FUTURE-MARITIME.pdf; Nineta Polemi, *Port Cybersecurity:*

Securing Critical Information Infrastructures and Supply Chains (Amsterdam, Elsevier, 2018).

156. Deloitte Port Services, "Smart Ports: Point of View," *Deloitte*, 2017, https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/energy-resources/deloitte-nl-er-port-services-smart-ports.pdf; Ahmadhon Kamolov and Su Hyun Park, "An IoT Based Smart Berthing (Parking) System for Vessels and Ports," in K. Kim and H. Kim (eds), *Mobile and Wireless Technology 2018, ICMWT 2018, Lecture Notes in Electrical Engineering* 513 (Singapore: Springer), https://doi.org/10.1007/978-981-13-1059-1_13.
157. Deloitte Port Services, 2017; Yongsheng Yang, Meisu Zhong, Haiqing Yao, Fang Yu, Xiuwen Fu, and Octavian Postolache, "Internet of Things for Smart Ports: Technologies and Challenges," *IEEE Instrumentation & Measurement Magazine* 21, no. 1 (February 2018): 34–43, https://doi.org/10.1109/MIM.2018.8278808.
158. Deloitte Port Services, 2017; Elisabeth van Opstall, "SmartPort: research and development for the port of Rotterdam," *Government Europa*, 10 September 2018, https://www.governmenteuropa.eu/smartport-port-of-rotterdam/90340/.
159. Abderrahmen Belfkih, Claude Duvallet, and Bruno Sadeg, "The Internet of Things For Smart Ports Application to the Port of Le Havre," in *Proceedings of Intelligent Platform for Smart Port* (IPaSPort) 2017, Normandie University, Le Havre, France (3–4 May 2017); Deloitte Port Services, 2017.
160. Stuxnet is described in appendix 5.
161. Andy Greenberg, "A Notorious Iranian Hacking Crew is Targeting Industrial Control Systems," *WIRED*, 28 November 2019, https://www.wired.com/story/iran-apt33-industrial-control-systems/; Greenberg, *SANDWORM*.
162. Jim Cooper, "Cyber Security Industrial Controls," in *Issues in Maritime Cyber Security*, ed. Joseph DiRenzo III, Nicole K. Drumhiller, and Fred S. Roberts (Washington, D.C.: Westphalia Press, 2017): 221–229; "Industrial Control System (ICS) Security," *PwC*, 2016, https://www.pwc.in/assets/pdfs/consulting/cyber-security/industrial-production/industrial-controls-system-ics-security.pdf; U.S. Department of Homeland Security, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," *Industrial Control Systems Cyber Emergency Response Team*, September 2016, https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.
163. George Leopold, "Military Enlists Digital Twin Technology to Secure Chips," *EE Times*, 2 January 2020, https://www.eetimes.com/military-enlists-digital-twin-technology-to-secure-chips/; Shaun Waterman, "Digital Twins Proliferate as Smart Way to Test Tech," *Air Force Magazine*, 15 March 2020, https://www.airforcemag.com/digital-twins-proliferate-as-smart-way-to-test-tech/.
164. Matthias Eckhart and Andreas Ekelhart, "Towards Security-Aware Virtual Environments for Digital Twins," CPSS '18: *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security* (May 2018): 61–72, https://doi.org/10.1145/3198458.3198464; Christos Koulamas and Athanasios Kalogeras,

"Cyber-Physical Systems and Digital Twins in the Industrial Internet of Things," *IEEE Computer Magazine* 51, no. 11 (November 2018): 95–98, https://doi.org/10.1109/MC.2018.2876181; Somayeh Malakuti and Sten Grüner, "Architectural Aspects of Digital Twins in IIoT Systems," *ECSA '18: Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings*, no. 12 (September 2018): 1–2, DOI: 10.1145/3241403.3241417.

165. "PROSTEP Builds Digital Twin to Optimise Shipbuilding," *Vessel Performance Optimisation*, 13 February 2020, https://vpoglobal.com/2020/02/13/prostep-builds-digital-twin-to-optimise-shipbuilding/.
166. Original quote: "The factory of the future will have only two employees, a man and a dog," https://www.brainyquote.com/quotes/warren_bennis_402360.
167. Andre Rose, "Cyber security concerns for autonomous and remotely controlled systems," *Riviera*, 6 May 2020, https://www.rivieramm.com/opinion/opinion/cyber-security-concerns-for-autonomous-and-remotely-controlled-systems-59261.
168. David Larter, "5 things you should know about the U.S. Navy's plans for autonomous missile boats," *Defense News*, 14 January 2020, https://news.yahoo.com/5-things-know-us-navy-225333042.html; "U.S. Navy Sea Hunter USV Will Operate With Carrier Strike Group," *Navy Recognition*, 22 January 2020, https://navyrecognition.com/index.php/news/defence-news/2020/january/7970-us-navy-sea-hunter-usv-will-operate-with-carrier-strike-group.html; "U.S. Navy's Ghost Fleet Overlord Unmanned Vessel Program Enters Next Phase," *Naval Today*, 2 October 2019, https://navaltoday.com/2019/10/02/us-navys-ghost-fleet-overlord-unmanned-vessel-program-enters-next-phase/.
169. U.S. Navy (USN), *The Navy Unmanned Surface Vehicle (USV) Master Plan*, U.S. Department of Defense, 23 July 2007, https://www.navy.mil/navydata/technology/usvmppr.pdf.
170. "U.S. Navy Tests Unmanned Patrol Boat for Port Security," *The Maritime Executive*, 13 February 2020, https://maritime-executive.com/article/u-s-navy-tests-unmanned-patrol-boat-for-port-security
171. Vishnu Rajamanickam, "The future of autonomous ships rests in their ability to tackle cyberattacks," *American Shipper*, 27 June 2019, https://www.freightwaves.com/news/the-future-of-autonomous-ships-rests-in-their-ability-to-tackle-cyberattacks.
172. Jeffery Mayger, "Autonomous Shipping—Cyber Hazards Ahead," *Marine News* 30, no. 10 (October 2019): 40–42, https://www.marinelink.com/news/autonomous-shipping-cyber-hazards-ahead-471587.
173. Matt Bishop, *Computer Security: Art and Science*, 2nd. ed. (Boston: Addison-Wesley, 2019); Mayger, 2019.
174. Sokratis K. Katsikas, "Cyber Security of the Autonomous Ship," in *CPSS '17: Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security* (April 2017): 55–56, https://doi.org/10.1145/3055186.3055191.

175. Kimberly Tam and Kevin Jones, "Cyber-Risk Assessment for Autonomous Ships," in *Proceedings of 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 11–12 June 2018, https://doi.org/10.1109/CyberSecPODS.2018.8560690.
176. See appendix 7 for a broader treatment of qualitative risk measurement and the Tam & Jones approach.
177. Kessler et al., "A Taxonomy Framework"; Ø.J. Rødseth and H.C. Burmeister, "Risk Assessment for an Unmanned Merchant Ship," *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation* 9, no. 3 (September 2015): 357–364, https://doi.org/10.12716/1001.09.03.08.
178. Bilhanan Silverajan, Mert Ocak, and Benjamin Nagel, "Cybersecurity Attacks and Defences for Unmanned Smart Ships," in *Proceedings of the 2018 IEEE Conferences on Internet of Things (iThings), Green Computing and Communications (GreenCom), Cyber, Physical and Social Computing (CPSCom), Smart Data (SmartData), Blockchain, Computer and Information Technology, Congress on Cybermatics*, Halifax, Nova Scotia, Canada (30 July–3 August 2018): 15–20, https://doi.org/10.1109/Cybermatics_2018.2018.00037.
179. Kessler et al., "A Taxonomy Framework"; Silverajan et al., "Cybersecurity Attacks and Defences."
180. Roger G. Johnston, "Security Maxims," *Right Brain Sekurity*, August 2019, 11, http://rbsekurity.com/Papers/Johnston%20Security%20Maxims.pdf.
181. Eckhart and Ekelhart, "Towards Security-Aware Virtual Environments"; "Keppel Developing"; Koulamas and Kalogeras, "Cyber-Physical Systems"; Malakuti and Grüner, "Architectural Aspects of Digital Twins."
182. https://www.goodreads.com/quotes/1269803-no-battle-plan-ever-survives-contact-with-the-enemy.
183. http://www.jewishmag.com/123mag/we_plan/we_plan.htm.
184. Lines spoken by Cosmo (Sir Ben Kingsley), *Sneakers* (Universal Pictures, 1992), https://www.imdb.com/title/tt0105435/quotes/?tab=qt&ref_=tt_trv_qu.
185. "The Maginot Line—11 Fascinating Facts About France's Great Wall," *MilitaryHistoryNow.com*, 7 May 2017, https://militaryhistorynow.com/2017/05/07/the-great-wall-of-france-11-remarkable-facts-about-the-maginot-line/.
186. Gary C. Kessler, "Security at the Speed of Thought," *Information Security Magazine*, November 2000, https://web.archive.org/web/20010211145859/http://infosecuritymag.com/articles/november00/columns_logoff.shtml; Zachary Staples and Maura Sullivan, "The Second Age of Cyber," *Fathom5*, 3 July 2018, https://c14d1d67-ab7e-43dc-a75b-79ac8837338a.filesusr.com/ugd/3d35e8_6f25f7bca8214cba8010c7a54e6c979a.pdf.
187. Rødseth and Burmeister, "Risk Assessment for an Unmanned."
188. "About Evergreen," *U.S. Coast Guard*, n.d., https://www.uscg.mil/Strategy/Evergreen/; Eric Popiel, "Evergreen Cyber Project," in *Issues in Maritime Cyber*

Security, ed. Joseph DiRenzo III, Nicole K. Drumhiller, and Fred S. Roberts (Washington, D.C.: Westphalia Press, 2017), 569–581.

189. Dave Bailey, "Why You Need to Follow the Steve Jobs Method and 'Work Backwards,'" *Inc*., 13 July 2017, https://www.inc.com/dave-bailey/why-you-need-to-follow-the-steve-jobs-method-and-w.html; Duncan Davidson, "Don't Try to be 'Disruptive.' To Really Have an Impact, You Need to Reverse Engineer the Future," 13 March 2018, https://www.entrepreneur.com/article/309552.
190. Anne Johnson and Emily Grumbling, Rapporteurs, *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop*, Computer Science and Telecommunications Board; Intelligence Community Studies Board; Division on Engineering and Physical Sciences; National Academies of Sciences, Engineering, and Medicine, 2019, https://doi.org/10.17226/25488.
191. Vego, "On Littoral Warfare"; Webb, *Introduction to Oceanography*.
192. Stewart, *Introduction to Physical Oceanography*; Webb, *Introduction to Oceanography*.
193. NovAtel, *Introduction to GNSS*.
194. Misra and Enge, *Global Positioning System*; NovAtel, *Introduction to GNSS*.
195. Misra and Enge, *Global Positioning System*; NovAtel, *Introduction to GNSS*.
196. 1 GHz = 1 gigahertz or 1 billion (10^9) cycles per second.
197. *Pseudorandom* means that the digital code appears to be random but, in fact, eventually starts to repeat after some period of time. If the period of time is very long, the pseudorandom code actually starts to take on characteristics of a totally random sequence. In GPS, the low precision PRN repeats every millisecond while the high precision PRN repeats about once a week (Misra and Enge, *Global Positioning System*).
198. Misra and Enge, *Global Positioning System*; NovAtel, *Introduction to GNSS*.
199. Misra and Enge, *Global Positioning System*; NovAtel, *Introduction to GNSS*.
200. Misra and Enge, *Global Positioning System*; NovAtel, *Introduction to GNSS*.
201. Misra and Enge, *Global Positioning System*; DOD, "Global Positioning System Precise Positioning Service Performance Standard," February 2007, https://www.gps.gov/technical/ps/2007-PPS-performance-standard.pdf; DOD, "Global Positioning System Standard Positioning Service Performance Standard," 4th Edition, September 2008, http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf; Whiting, "GPS Celebrates."
202. GPS.gov, "Selective Availability," 27 September 2018, https://www.gps.gov/systems/gps/modernization/sa/.
203. Misra and Enge, *Global Positioning System*; DOD, "GPS Precise Positioning Service"; DOD, "GPS Standard Positioning Service."
204. 1 MHz = 1 megahertz or 1 million (10^6) cycles per second.
205. Global Positioning Systems (GPS) Directorate, "Systems Integration & Engineering Interface Specification," IS-GPS-200J, 25 April 2018, https://www.gps.gov/technical/icwg/IS-GPS-200J.pdf; GPS.gov, "Space Segment," 26 November 2019,

https://www.gps.gov/systems/gps/space/; Misra and Enge, *Global Positioning System*; NovAtel, *Introduction to GNSS*; DOD, "GPS Precise Positioning Service"; DOD, "GPS Standard Positioning Service."

206. Global Positioning Systems (GPS) Directorate, 2018; Misra and Enge, *Global Positioning System*; NovAtel, *Introduction to GNSS*; DOD, "GPS Precise Positioning Service"; DOD, "GPS Standard Positioning Service."
207. Misra and Enge, *Global Positioning System*; NovAtel, *Introduction to GNSS*; DOD, "GPS Standard Positioning Service."
208. To be a little more technically complete, the signal is composed by modulating the carrier frequency with a bit string composed of the navigation message bit string *exclusively ORed* with the satellite's unique PRN code bit string (i.e., if two input bits are the same, the result is a 0 and if two input bits are different, the result is a 1). The PPS signal is sent 90° out-of-phase from the SPS signal. See Misra and Enge, *Global Positioning System*.
209. GPS.gov, "Space Segment"; Misra and Enge, *Global Positioning System*; NovAtel, *Introduction to GNSS*; DOD, "GPS Standard Positioning Service."
210. GPS.gov, "Space Segment"; Misra and Enge, *Global Positioning System*; NovAtel, *Introduction to GNSS*; DOD, "GPS Standard Positioning Service."
211. National Marine Electronics Association (NMEA), "NMEA 0183 Interface Standard," 2019, https://www.nmea.org/content/STANDARDS/NMEA_0183_Standard.
212. Coordinated Universal Time, aka Universal Time Coordinated *or* Zulu.
213. Dale DePriest, "NMEA Data," n.d., https://www.gpsinformation.org/dale/nmea.htm; Eric S. Raymond, "NMEA Revealed," version 2.23, March 2019, https://gpsd.gitlab.io/gpsd/NMEA.html.
214. Kimbra Cutlip, "AIS for Safety and Tracking: A Brief History," *Global Fishing Watch*, 31 March 2017, https://globalfishingwatch.org/data/ais-for-safety-and-tracking-a-brief-history; International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), *An Overview of AIS* (Edition 2), IALA Guideline 1082, June 2016, https://www.navcen.uscg.gov/pdf/IALA_Guideline_1082_An_Overview_of_AIS.pdf.
215. U.S. Code of Federal Regulations, Title 33, Chapter I, Part 164—Navigation Safety Regulations, Section 46—Automatic Identification System (33 CFR 164.46), https://www.govregs.com/regulations/33/164.46.
216. International Maritime Organization (IMO), *International Convention for the Safety of Life at Sea (SOLAS)*, "Chapter V (Safety of Navigation), Regulation 19 (Carriage requirements for shipborne navigational systems and equipment)," 1 July 2002, https://mcanet.mcga.gov.uk/public/c4/solas/index.html; U.S. Coast Guard (USCG), "AIS Requirements," USCG Navigation Center website, 14 August 2019, https://www.navcen.uscg.gov/?pageName=AISRequirementsRev.
217. IALA, *An Overview of AIS*.
218. Cutlip, "AIS for Safety"; IALA, *An Overview of AIS*.

219. Cutlip, "AIS for Safety."

220. International Telecommunication Union (ITU), *Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band*, "ITU-R Recommendation M.1371-5. M Series: Mobile, radiodetermination, amateur and related satellite services," February 2014, https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1371-5-201402-I!!PDF-E.pdf; ITU, *Assignment and use of identities in the maritime mobile service*, "ITU-R Recommendation M.585-8. M Series: Mobile, radiodetermination, amateur and related satellite services," October 2019, https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.585-8-201910-I!!PDF-E.pdf.

221. ITU Rec. M.585; USCG, "Maritime Mobile Service Identity," https://www.navcen.uscg.gov/index.php ?pageName=mtMmsi.

222. NMEA, "NMEA 0183"; Eric S. Raymond, "AIVDM/AIVDO Protocol Decoding," version 1.54, November 2019, https://gpsd.gitlab.io/gpsd/AIVDM.html.

223. NMEA, "NMEA 2000® Interface Standard," 2019, https://www.nmea.org/content/STANDARDS/NMEA_2000.

224. NMEA, "OneNet Standard."

225. Dictionary.com, "Cybersecurity," https://www.dictionary.com/browse/cybersecurity; Digital Guardian, "A Definition of Cyber Security," https://digitalguardian.com/blog/what-cyber-security; Merriam-Webster, "Cybersecurity," https://www.merriam-webster.com/dictionary/cybersecurity.

226. DOD, *Dictionary of Military Terms*, 62. Also note that integrity, authentication, confidentiality, and nonrepudiation are key requirements for use of cryptography, further discussion of which is beyond the scope of this monograph—see Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, *Cryptography Engineering: Design Principles and Practical Applications* (New York: John Wiley & Sons, Inc., 2010); Gary C. Kessler, "An Overview of Cryptography," 1 June 2020, https://www.garykessler.net/library/crypto.html.

227. The DOD terminology is specific and purposeful. While many in the industry argue that cybersecurity is a subset of information assurance and others argue the opposite, DOD makes it clear that *cybersecurity* supersedes *information assurance*, and that the two terms are neither synonyms nor interchangeable. See U.S. Navy, "DOD Instructions Lead to Change in Cybersecurity Term," Chief Information Officer, 25 August 2014, https://www.doncio.navy.mil/ContentView.aspx?ID=5431.

228. Donn B. Parker, "Toward a New Framework for Information Security?,"in S. Bosworth, M.E. Kabay, and E. Whyne, ed., *Computer Security Handbook*, 6th ed. (Hoboken, NJ: John Wiley & Sons, Inc., 2015).

229. Cisco Systems, "What is Malware?," n.d., https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html; Malwarebytes, "Malware," n.d., https://www.malwarebytes.com/malware/; Merriam-Webster, "Malware," n.d., https://www.merriam-webster.com/dictionary/malware.

230. Shawn Abraham, "List of Types of Malware," *MalwareFox*, 1 August 2019, https://www.malwarefox.com/malware-types/; David Kim and Michael G. Solomon, *Fundamentals of Information Systems Security*, 3rd. ed. (Burlington, MA: Jones & Bartlett Learning, 2018); Michael E. Whitman and Herbert J. Mattord, *Principles of Information Security*, 6th. ed. (Boston: Cengage Learning, 2018).
231. Kim and Solomon, *Fundamentals of Information Systems Security*; Whitman and Mattord, *Principles of Information Security*.
232. Peter J. Denning, "The Internet Worm," Research Institute for Advanced Computer Science (RIACS) Technical Report TR-89.3, 7 February 1989, https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19900014594.pdf; Joyce Reynolds, "The Helminthiasis of the Internet," Network Working Group, Request for Comments (RFC) 1135, December 1989, https://www.rfc-editor.org/rfc/rfc1135.
233. Abraham, "List of Types"; Kim and Solomon, *Fundamentals of Information Systems Security*; Whitman and Mattord, *Principles of Information Security*.
234. Abraham, "List of Types"; Kim and Solomon, *Fundamentals of Information Systems Security*; Whitman and Mattord, *Principles of Information Security*.
235. Christine Howler, "Remove CoinTicker Malware from Mac," *HowToRemove.Guide*, October 2018, https://howtoremove.guide/remove-cointicker-mac/.
236. Mark Mazzetti, Nicole Perlroth, and Ronen Bergman, "It Seemed Like a Popular Chat App. It's Secretly a Spy Tool," *The New York Times*, 22 December 2019, https://www.nytimes.com/2019/12/22/us/politics/totok-app-uae.html; Steven Musil, "Popular Messaging App ToTok Reportedly an Emirati Spy Tool," *CNET*, 22 December 2019, https://www.cnet.com/news/popular-messaging-app-totok-reportedly-an-emirati-spy-tool/; M.B. Pell and Echo Wang, "U.S. Navy Bans TikTok From Government-Issued Mobile Devices," 20 December 2019, https://www.reuters.com/article/us-usa-tiktok-navy-idUSKBN1YO2HU; Queenie Wong, "TikTok Accused of Secretly Gathering User Data and Sending it to China," *CNET*, 2 December 2019, https://www.cnet.com/news/tiktok-accused-of-secretly-gathering-user-data-and-sending-it-to-china/.
237. Hak5, "O.MG Cable," 2020, https://shop.hak5.org/products/o-mg-cable; Joseph Cox, "These Legit-Looking iPhone Lightning Cables Will Hijack Your Computer," *Motherboard Tech by Vice*, 10 August 2019, https://www.vice.com/en_us/article/evj4qw/these-iphone-lightning-cables-will-hack-your-computer; Joseph Cox, "Legit-Looking iPhone Lightning Cables That Hack You Will be Mass Produced and Sold," Motherboard Tech by *Vice*, 30 September 2019, https://www.vice.com/en_us/article/3kx5nk/fake-apple-lightning-cable-hacks-your-computer-omg-cable-mass-produced-sold.
238. KnowBe4, Inc., "What is Phishing?," n.d., https://www.phishing.org/what-is-phishing; Kim and Solomon, *Fundamentals of Information Systems Security*; Zulfikar Ramzan, "Phishing attacks and countermeasures," In Mark Stamp and Peter Stavroulakis (eds.), *Handbook of Information and Communication Security* (Berlin: Springer-Verlag, 2010); Whitman and Mattord, *Principles of Information Security*.

239. Kim and Solomon, *Fundamentals of Information Systems Security*; KnowBe4, "What is Phishing?"; Ramzan, "Phishing attacks and countermeasures"; Whitman and Mattord, *Principles of Information Security*.
240. The DNS is the distributed internet database that, among other things, translates host names (e.g., *www.socom.mil*) to IP addresses (e.g., *209.22.230.8*). If the DNS is compromised, users cannot get access to web and other internet servers based upon host names.
241. In one attack scenario, malware is used to infect a local computer's *hosts* file which contains a mapping of host names to IP addresses.
242. Kim and Solomon, *Fundamentals of Information Systems Security*; KnowBe4, "What is Phishing?"; Ramzan, "Phishing attacks and countermeasures"; Whitman and Mattord, *Principles of Information Security*.
243. Kim and Solomon, *Fundamentals of Information Systems Security*; KnowBe4, "What is Phishing?"; Ramzan, "Phishing attacks and countermeasures"; Whitman and Mattord, *Principles of Information Security*.
244. Kim and Solomon, *Fundamentals of Information Systems Security*; KnowBe4, "What is Phishing?"; Ramzan, "Phishing attacks and countermeasures"; Whitman and Mattord, *Principles of Information Security*.
245. Dhirag Ranka, "Inside Dalai Lama Website Attacks: Analyzing the 'Watering Hole Attacks,'" *Network Intelligence*, 5 September 2013, https://niiconsulting.com/checkmate/2013/09/inside-dalai-lama-website-attacks-analyzing-watering-hole-attacks/; Symantec Security Response, "Internet Explorer Zero-Day Used in Watering Hole Attack: Q&A," *Symantec Official Blog*, 31 December 2012, https://www.symantec.com/connect/blogs/internet-explorer-zero-day-used-watering-hole-attack-qa.
246. When internet client software (e.g., a browser) initiates a connection with an internet server (e.g., a web server), the client and server engage in what is called a *three-way handshake* to set up the logical channel. The client starts with the request. The server responds by allocating some memory space for the connection and giving the client some information needed to complete the setup. The client now completes the connection request so that the client and server can properly exchange data. The entire three-way handshake usually takes less than a second. In this form of DoS attack, the client deliberately does not perform the third step, so the server sits and waits, possibly in excess of 10 seconds, before it deallocates the memory buffer. In the Panix attack, there were 150 unanswered connection requests every second, so the servers quickly ran out of memory.
247. Steven Cherry, "Panix Attack: How New York City's Oldest Internet Service Provider was Hijacked and Rescued," *IEEE Spectrum*, 1 February 2005, https://spectrum.ieee.org/telecom/security/panix-attack.
248. Radware, "History of DDoS Attacks," 13 March 2017, https://security.radware.com/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/.
249. Carlos Morales, "Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us," *NETSCOUT*, 5 March 2018, https://www.netscout.com/blog/asert/

netscout-arbor-confirms-17-tbps-ddos-attack-terabit-attack-era; Iain Thomson, "World's Biggest DDoS Attack Record Broken After Just Five Days," *The Register*, 5 March 2018, https://www.theregister.co.uk/2018/03/05/worlds_biggest_ddos_attack_record_broken_after_just_five_days/; 1 Tbps = 1 terabit per second = 1 trillion (10^{12}) bits per second.

250. Dormando, "What is Memcached?," 2018, https://www.memcached.org/; Dormando, "memcached," 11 November 2019, https://github.com/memcached/memcached.

251. 1 MB = 1 megabyte = 1 million (10^6) bytes.

252. Abraham, "List of Types"; Kim and Solomon, *Fundamentals of Information Systems Security*; Whitman and Mattord, *Principles of Information Security*.

253. Brian Krebs, "Powerful New DDoS Method Adds Extortion," *Krebs on Security*, 2 March 2018, https://krebsonsecurity.com/2018/03/powerful-new-ddos-method-adds-extortion/; Cybereason Security Team, "Attackers Include Ransom Note in Amplified DDoS Attacks that use memcached Servers," *Cybereason*, https://www.cybereason.com/blog/memcached-ddos-attack.

254. Kevin Collier, "Crippling Ransomware Attacks Targeting U.S. Cities on the Rise," *CNN*, 10 May 2019, https://www.cnn.com/2019/05/10/politics/ransomware-attacks-us-cities/index.html.

255. Jon Clay, "This Week in Security News: Ransomware Campaigns and Cryptocurrency Miners," 1 August 2019, https://blog.trendmicro.com/this-week-in-security-news-ransomware-campaigns-and-cryptocurrency-miners/.

256. Cisco, "What is an Advanced Persistent Threat (APT)?," n.d., https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html; Sarah Maloney, "What is an Advanced Persistent Threat (APT)?," *Cybereason*, 9 January 2018, https://www.cybereason.com/blog/advanced-persistent-threat-apt.

257. ITgovernance, "Advanced Persistent Threats (APTs)," n.d., https://www.itgovernance.co.uk/advanced-persistent-threats-apt.

258. Mandiant, "APT1: Exposing One of China's Espionage Units," 18 February 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

259. Ariana Eunjung Cha and Ellen Nakashima, "Google China Cyberattack Part of Vast Espionage Campaign, Experts Say," *The Washington Post*, 14 January 2010, https://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html; Google, "A New Approach to China," Official blog, 12 January 2010, https://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

260. International Association of Chiefs of Police (IACP), "Cyber Attack Lifecycle," *Law Enforcement Cyber Center*, n.d., https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/; Mandiant, 2013.

261. FireEye, "What is a Zero-Day Exploit?," n.d., https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html; Kim Zetter, *Countdown to Zero Day:*

Stuxnet and the Launch of the World's First Digital Weapon (New York: Crown, 2014).

262. Cha and Nakashima, "Google China Cyberattack"; Google, "A New Approach."
263. Serge Egelman, Cormac Herley, and Paul C. van Oorschot, "Markets For Zero-Day Exploits: Ethics and Implications," *New Security Paradigms Workshop (NSPW) '13*, 9–12 September 2013, 41–46, https://doi.org/10.1145/2535813.2535818; Lily Hay Newman, "Feds Explain Their Software Bug Stash—But Don't Erase Concerns," *WIRED*, 15 November 2017, https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns/; Zetter, *Countdown to Zero Day*.
264. Sam Biddle, "The NSA Leak is Real, Snowden Documents Confirm," *The Intercept*, 19 August 2016, https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/; Henry Farrell, "Hackers Have Just Dumped a Treasure Trove of NSA Data. Here's What it Means," *The Washington Post*, 15 April 2017, https://www.washingtonpost.com/news/monkey-cage/wp/2017/04/15/shadowy-hackers-have-just-dumped-a-treasure-trove-of-nsa-data-heres-what-it-means/; Greenberg, SANDWORM; Krebs, "WikiLeaks Dumps Docs"; WikiLeaks, "Vault 7: Projects," 2017, https://wikileaks.org/vault7/index.html; It should be noted that the NSA does not weaponize every vulnerability that it finds—as a case in point, see National Security Agency (NSA), "Patch Critical Cryptographic Vulnerability in Microsoft Windows Clients and Servers," *Cybersecurity Advisory*, 14 January 2020, https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF.
265. With apologies to The Wizard of Oz ("Lions and tigers and bears, oh my!").
266. NIST, "Framework for Cyber-Physical Systems."
267. Graham Williamson, "OT, ICS, SCADA—What's the difference?," *Kuppinger-Cole Analysts*, 7 July 2015, https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference.
268. Brendan Galloway and Gerhard P. Hancke, "Introduction to Industrial Control Networks," *IEEE Communications Surveys & Tutorials* 15, no. 2 (Second Quarter, 2013): 860–880; Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn, "Guide to Industrial Control Systems (ICS) Security," rev. 2, National Institute of Standards and Technology (NIST) Special Publication 800-82, U.S. Department of Commerce, May 2015, http://doi.org/10.6028/NIST.SP.800-82r2; Williamson, "OT, ICS, SCADA."
269. Galloway and Hancke, "Introduction to Industrial Control Networks"; Stouffer et al., "Guide to ICS"; Williamson, "OT, ICS, SCADA."
270. Stouffer et al., "Guide to ICS."
271. Stouffer et al., "Guide to ICS."
272. Stouffer et al., "Guide to ICS"; Unitronics, "What is the Definition of 'PLC'?," n.d., https://unitronicsplc.com/what-is-plc-programmable-logic-controller/; Sadegh vosough and Amir vosough, "PLC and its Applications," *International Journal*

of Multidisciplinary Sciences and Engineering 2, no. 8 (November 2011): 41–46, http://www.ijmse.org/Volume2/Issue8/paper9.pdf.

273. Sivaranjith, "PLC vs. DCS, Difference Between PLC and DCS," *AutomationForum.co*, 20 August 2019, https://automationforum.co/what-are-difference-between-plc-labview-and-dcs/; Stouffer et al., "Guide to ICS"; The Engineering Concepts, "What is Distributed Control Systems (DCS)?," *Engineering Concepts*, 26 December 2018, https://www.theengineeringconcepts.com/what-is-distributed-control-systems-dcs/.

274. Vidya Muthukrishnan, "SCADA System: What is it? (Supervisory Control and Data Acquisition)," *Electrical 4 U*, 14 January 2020, https://www.electrical4u.com/scada-system/; Stouffer et al., "Guide to ICS"; Williamson, "OT, ICS, SCADA."

275. Galloway and Hancke, "Introduction to Industrial Control Networks"; Ben Joan, "Difference Between DCS and SCADA," *DifferenceBetween.net*, n.d., http://www.differencebetween.net/technology/difference-between-dcs-and-scada/; Stouffer et al., "Guide to ICS"; Williamson, "OT, ICS, SCADA."

276. Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo, "Cyber-Physical Systems Security—A Survey," *IEEE Internet of Things Journal* 4, no. 6 (December 2017): 1802–1831, https://doi.org/10.1109/JIOT.2017.2703172; Stouffer et al., "Guide to ICS"; Eric Ke Wang, Yunming Ye, Xiaofei Xu, S.M. Yiu, L.C.K. Hui, and K.P .Chow, "Security Issues and Challenges for Cyber Physical System," in *Proceedings of 2010 IEEE/ACM International Conference on Green Computing and Communications & 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing* (18–20 December 2010): 733–738, https://doi.org/10.1109/GreenCom-CPSCom.2010.36.

277. Ironically, the details of the Aurora Generator Test were inadvertently shared by DHS in response to a request for information about the Chinese hack on Google—called Operation Aurora—that occurred in 2009. See Curtis Waltman, "Aurora: Homeland Security's Secret Project to Change How We Think About Cybersecurity," *Muckrock*, 14 November 2016, https://www.muckrock.com/news/archives/2016/nov/14/aurora-generator-test-homeland-security/.

278. Greenberg, *SANDWORM*; U.S. Department of Homeland Security (DHS), "Challenges Remain in DHS' Efforts to Secure Control Systems," *Office of Inspector General*, OIG-09-95, August 2009, https://www.oig.dhs.gov/assets/Mgmt/OIG_09-95_Aug09.pdf; Waltman, "Aurora"; Zetter, *Countdown to Zero Day*; "Staged Cyber Attack Reveals Vulnerability in Power Grid," *CNN* (video), https://www.youtube.com/watch?v=fJyWngDco3g.

279. David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum* 50, no. 3 (March 2013): 48–53, https://doi.org/10.1109/MSPEC.2013.6471059; Greenberg, *SANDWORM*; Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *WIRED*, 3 November 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/; Zetter, *Countdown to Zero Day*.

280. Dragos, "TRISIS Malware: Analysis of Safety System Targeted Malware," version 1.20171213, 13 December 2017, https://dragos.com/wp-content/uploads/

TRISIS-01.pdf; Andy Greenberg, "'Crash Override': The Malware That Took Down a Power Grid," *WIRED*, 12 June 2017, https://www.wired.com/story/crash-override-malware/; US-CERT, "CRASHOVERRIDE Malware," ICS Alert (ICS-ALERT-17-206-01), *Cybersecurity & Infrastructure Security Agency (CISA), U.S. Department of Homeland Security*, 25 July 2017, https://www.us-cert.gov/ics/alerts/ICS-ALERT-17-206-01.

281. Bjorn Fehrm, "Boeing's automatic trim for the 737 MAX was not disclosed to the Pilots," *Leeham News*, 14 November 2018, https://leehamnews.com/2018/11/14/boeings-automatic-trim-for-the-737-max-was-not-disclosed-to-the-pilots/; Ministry of Transport, "Aircraft Accident Investigation Preliminary Report, Ethiopian Airlines Group B737-8 (MAX) Registered ET-AVJ, 28 NM South East of Addis Ababa, Bole International Airport, March 10, 2019," Report No. AI-01/19, *Federal Democratic Republic of Ethiopia, Aircraft Accident Investigation Bureau*, April 2019, https://flightsafety.org/wp-content/uploads/2019/04/Preliminary-Report-B737-800MAX-ET-AVJ.pdf.

282. Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi, "Internet of Things Security: A Survey," *Journal of Network and Computer Applications* 88 (15 June 2017): 10–28, https://doi.org/10.1016/j.jnca.2017.04.002; Elisa Bertino and Nayeem Islam, "Botnets and Internet of Things Security," *IEEE Computer Magazine* 50, no. 2 (February 2017): 76–79, https://doi.org/10.1109/MC.2017.62; Djamel Eddine Kouicem, Abdelmadjid Bouabdallah, and Hicham Lakhlef, "Internet of Things Security: A Top-Down Survey," *Computer Networks* 141 (4 August 2018): 199–221; J. Sathish Kumar and Dhiren R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," *International Journal of Computer Applications* 90, no. 11 (March 2014): 20–26.

283. Federal Bureau of Investigation (FBI), "Common Internet of Things Devices May Expose Consumers to Cyber Exploitation," Public Service Announcement Alert No. I-101717a-PSA, 17 October 2017, https://www.ic3.gov/media/2017/171017-1.aspx.

284. For examples, see Censys (https://censys.io/) or Shodan (https://www.shodan.io/).

285. Catalin Cimpanu, "Hacker leaks passwords for more than 500,000 servers, routers, and IoT devices," *ZDNet*, 19 January 2020, https://www.zdnet.com/article/hacker-leaks-passwords-for-more-than-500000-servers-routers-and-iot-devices/; SafeGadget, "Hacked Internet of Things Database - Gadgets, Cameras, Wireless Routers," 26 June 2019, https://www.safegadget.com/139/hacked-internet-things-database/.

286. Julian Assange is the founder of WikiLeaks. After an international arrest warrant was issued in 2010, Assange eventually sought asylum in Ecuador, which is where he was in 2016.

287. Scott Hilton, "Dyn Analysis Summary Of Friday October 21 Attack," *Dyn*, 26 October 2016, https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/; Lily Hay Newman, "What We Know About Friday's Massive East Coast Internet Outage," *WIRED*, 21 October 2016, https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/; Bruce Schneier, "Lessons From the Dyn DDoS

Attack," *Security Intelligence*, 1 November 2016, https://securityintelligence.com/lessons-from-the-dyn-ddos-attack/.

288. Bertino and Islam, "Botnets and Internet of Things"; Brian Krebs, "KrebsOnSecurity Hit With Record DDoS," *Krebs on Security*, 21 September 2016, https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/; Pierluigi Paganini, "OVH Hosting Hit by 1 Tbps DDoS Attack, the Largest One Ever Seen," *Security Affairs*, 25 September 2016, http://securityaffairs.co/wordpress/51640/cyber-crime/tbps-ddos-attack.html; Bernhard Rinner, "Can We Trust Smart Cameras?," *IEEE Computer Magazine* 52, no. 5 (May 2019): 67–70, https://doi.org/10.1109/MC.2019.2905171.
289. Jaime Pancorbo Crespo, Luis Guerrero Gómez, and Javier González Arias, "Autonomous Shipping and Cybersecurity," *Ship Science & Technology* 13, no. 25 (July 2019): 19–26, https://doi.org/10.25043/19098642.185; Katsikas, "Cyber Security."
290. "Cruise Ship Piloted Remotely During Sea Trials," *SAFETY4SEA*, 21 May 2020, https://safety4sea.com/cruise-ship-piloted-remotely-during-sea-trials/; Jasmina Ovcina, "De Hoop Conducts Remotely-Operated Sea Trials for Silver Origin," *Offshore Energy*, 22 May 2020, https://www.offshore-energy.biz/de-hoop-conducts-remotely-operated-sea-trials-for-silver-origin/.
291. "Autonomous Ships and Their Impact," *Opensea.pro Blog*, n.d., https://opensea.pro/blog/automated-ships; Crespo et al., "Autonomous Shipping and Cybersecurity"; Esa Jokioinen et al., "Remote and Autonomous Ships: The Next Steps," *Advanced Autonomous Waterborne Applications (AAWA)*, June 2016, https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf; Lech Kobyliński, "Smart Ships—Autonomous or Remote Controlled?," *Scientific Journals of the Maritime University of Szczecin* 53, no. 125 (March 2018): 28–34, https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-f98383e2-a4e3-4786-8c5a-2ad5117234c7/c/kobylinski_Smart_ships_53-2018.pdf; Oskar Levander, "Autonomous Ships on the High Seas," *IEEE Spectrum* 54 , no. 2 (February 2017): 26–31, https://doi.org/10.1109/MSPEC.2017.7833502.
292. Dyllan Furness, "Autonomous ships are coming, and we're not ready for them," *Digital Trends*, 13 July 2019, https://www.digitaltrends.com/cool-tech/autonomous-ships-are-coming/; Levander, "Autonomous Ships"; Jon Walker, "Autonomous Ships Timeline—Comparing Rolls-Royce, Kongsberg, Yara and More," *Emerj*, 22 November 2019, https://www.techemergence.com/autonomous-ships-timeline/.
293. There is a saying, at least among captains of small boats operating in near coastal waters, that "Driving a boat is the simplest thing in the world … until it's not."
294. "Autonomous Ships and Their Impact"; Furness, "Autonomous ships are coming"; Kobyliński, "Smart Ships"; Levander, "Autonomous Ships"; Ørnulf Jan Rødseth, "From Concept to Reality: Unmanned Merchant Ship Research in Norway," in *Proceedings of 2017 IEEE Underwater Technology (UT)*, 21–24 February 2017,

Busan, S. Korea, https://doi.org/10.1109/UT.2017.7890328; Walker, "Autonomous Ships Timeline."

295. Levander, "Autonomous Ships"; Walker, "Autonomous Ships Timeline."
296. "Autonomous Ships and Their Impact"; Levander, "Autonomous Ships"; Rødseth, "From Concept to Reality."
297. International Maritime Organization (IMO), "International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW)," 25 June 2010, http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-on-Standards-of-Training,-Certification-and-Watchkeeping-for-Seafarers-(STCW).aspx; Kobyliński, "Smart Ships."
298. Thomas Porathe, "Safety of Autonomous Shipping: COLREGS and Interaction Between Manned and Unmanned Ships," Edited by Michael Beer and Enrico Zio (eds.), *Proceedings of the 29th European Safety and Reliability Conference* (2019): 4146–4153, http://rpsonline.com.sg/proceedings/9789811127243/html/0655.xml; United States Coast Guard (USCG), *Navigation Rules: International—Inland*, COMDTINST M16672.2D, U.S. Department of Homeland Security, April 2004, https://www.navcen.uscg.gov/pdf/navRules/navrules.pdf.
299. "Autonomous Ships and Their Impact"; Jokioinen et al., "Remote and Autonomous Ships"; Walker, "Autonomous Ships Timeline"; "Welcome to the MUNIN Project Web Page," *MUNIN*, 2016, http://www.unmanned-ship.org/munin/.
300. Jokioinen et al., "Remote and Autonomous Ships"; Rødseth, "From Concept to Reality."
301. "USS Cole Attacked by Terrorists," *History*, 27 July 2019, https://www.history.com/this-day-in-history/uss-cole-attacked-by-terrorists.
302. "Welcome to the MUNIN Project."
303. Esa Jokioinen, "Advanced Autonomous Waterborne Applications (AAWA) Initiative," *The Connected Ship and Shipping Conference*, Brussels, 29 June 2016, https://www.waterborne.eu/media/18556/Advanced-Autonomous-Waterborne-Applications-AAWA-Initiative.pdf; "Rolls-Royce to Lead Autonomous Ship Research Project," *Rolls-Royce*, 2 July 2015, https://www.rolls-royce.com/media/press-releases/2015/pr-02-07-15-rolls-royce-to-lead-autonomous-ship-research-project.aspx.
304. "Japanese Consortium to Develop Autonomous Ocean Transport System," *World Maritime News*, 26 May 2017, https://worldmaritimenews.com/archives/221013/japanese-consortium-to-develop-autonomous-ocean-transport-system/; Walker, "Autonomous Ships Timeline."
305. Crespo et al., "Autonomous Shipping and Cybersecurity"; "NOVIMAR and the Vessel Train Concept," *NOVIMAR VesselTrain*, n.d., https://novimar.eu/concept/.
306. Jason Jiang, "Kongsberg and Wilhelmsen form the world's first autonomous shipping line," *Splash 247*, 4 April 2018, https://splash247.com/kongsberg-wilhelmsen-set-autonomous-shipping-jv/; "Kongsberg and Wilhelmsen Launch Autonomous-Shipping JV," *The Maritime Executive*, 3 April 2018, https://www.

maritime-executive.com/article/kongsberg-and-wilhelmsen-launch-autonomous-shipping-jv.

307. Aaron Chong, "Autonomous Ships in Singapore Could Become a Reality With MPA's New Innovation Lab," *Channel News Asia*, 9 April 2019, https://www.channelnewsasia.com/news/singapore/autonomous-ships-in-singapore-could-become-a-reality-with-mpa-s-11425762.

308. Rolls-Royce's Commercial Marine was acquired by Kongsberg Maritime in April 2019.

309. "Falco makes world's first autonomous ferry crossing," *The Engineer*, 3 December 2018, https://www.theengineer.co.uk/falco-autonomous-ferry-rolls-royce/; Bernard Marr, "The Incredible Autonomous Ships Of The Future: Run By Artificial Intelligence Rather Than A Crew," *Forbes*, 5 June 2019, https://www.forbes.com/sites/bernardmarr/2019/06/05/the-incredible-autonomous-ships-of-the-future-run-by-artificial-intelligence-rather-than-a-crew/#441cadf16fbf.

310. "Automatic Ferry Enters Regular Service Following World-First Crossing With Passengers Onboard," *Kongsberg Maritime*, 13 February 2020, https://www.kongsberg.com/maritime/about-us/news-and-media/news-archive/2020/first-adaptive-transit-on-bastofosen-vi/; Malcolm Latarche, "Automatic Ferry First Claimed by Kongsberg," *ShipInsight*, 13 February 2020, https://shipinsight.com/articles/automatic-ferry-first-claimed-by-kongsberg.

311. Eric Haun, "Yara Birkeland Project Paused Due to COVID-19," *MarineLink*, 11 May 2020, https://www.marinelink.com/news/yara-birkeland-project-paused-due-covid-478386; Asle Skredderberget, "The First Ever Zero Emission, Autonomous Ship," *Yara*, 14 March 2018, https://www.yara.com/knowledge-grows/game-changer-for-the-environment/; Marr, 2019; Walker, "Autonomous Ships Timeline."

312. Mark Anderson, "Bon Voyage for the Autonomous Ship *Mayflower*," *IEEE Spectrum*, 3 January 2020, https://spectrum.ieee.org/energy/renewables/bon-voyage-for-the-autonomous-ship-mayflower; Darrell Etherington, "Autonomous 'Mayflower' research ship will use IBM AI tech to cross the Atlantic in 2020," *TechCrunch*, 16 October 2019, https://techcrunch.com/2019/10/16/autonomous-mayflower-research-ship-will-use-ibm-ai-tech-to-cross-the-atlantic-in-2020/; "IBM Boards the *Mayflower* Autonomous Ship Project," *IBM*, 16 October 2019, https://newsroom.ibm.com/2019-10-16-IBM-Boards-the-Mayflower-Autonomous-Ship-Project; Brett Phaneuf, "Mayflower: How I Came to Build an Autonomous Ship to Cross the Atlantic," *IBM*, 16 October 2019, https://www.ibm.com/blogs/think/2019/10/rethinking-the-mayflower/.

313. Henk Hensen, Johan de Jong, Markus van der Laan, and Daan Merkelbach, "The Road Towards Autonomous Ship Handling with Tugs," *SWZ Maritime*, 7 November 2019, https://www.swzmaritime.nl/news/2019/07/11/the-road-towards-autonomous-ship-handling-with-tugs/.

314. Nick Blenkey, "ABB, Keppel Cooperate on Autonomous Tug for Singapore Ops," *MarineLog*, 21 October 2019, https://www.marinelog.com/coastal/tugs-barges/

abb-keppel-cooperate-on-autonomous-tug-for-singapore-ops/; Hensen et al., "The Road Towards"; "Keppel Developing Autonomous Tugboat," *Offshore*, 10 April 2019, https://www.offshore-mag.com/rigs-vessels/article/16790823/keppel-developing-autonomous-tugboat.

315. Rob O'Dwyer, "Automated Mooring System Chosen for Autonomous Container System," *Smart Maritime Network*, 13 June 2019, https://smartmaritimenetwork.com/2019/06/13/automated-mooring-system-chosen-for-autonomous-container-ship/.
316. Tor A. Johansen and Tristan Perez, "Unmanned Aerial Surveillance System For Hazard Collision Avoidance In Autonomous Shipping," in *Proceedings of 2016 International Conference on Unmanned Aircraft Systems* (ICUAS), 7–10 June 2016 (Arlington, VA), https://doi.org/10.1109/ICUAS.2016.7502542.
317. "Optimising ship inspections with autonomous drones," *Vessel Performance Optimisation*, 24 January 2020, https://vpoglobal.com/2020/01/24/optimising-ship-inspections-with-autonomous-drones/.
318. Hensen et al., "The Road Towards."
319. Vyacheslav Kharchenko and Volodymyr Torianyk, "Cybersecurity of the Internet of Drones: Vulnerabilities Analysis and IMECA Based Assessment," in *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies* (DESSERT), Kiev, Ukraine (24–27 May 2018), https://doi.org/10.1109/DESSERT.2018.8409160; B. Siddappaji and K.B. Akhilesh, "Role of Cyber Security in Drone Technology," in *Smart Technologies*, ed. Akhilesh K. and Möller D. (Singapore: Springer, 2020): 169–178, https://doi.org/10.1007/978-981-13-7139-4_13.
320. Gary C. Kessler, "Cybersecurity and the 'Return on Negligence,'" *Maritime Executive*, 12 October 2018, https://www.maritime-executive.com/editorials/cybersecurity-and-the-return-on-negligence; Kim and Solomon, *Fundamentals of Information Systems Security*; Whitman and Mattord, *Principles of Information Security*.
321. Kessler et al., "A Taxonomy Framework"; Kim and Solomon, *Fundamentals of Information Systems Security*; Whitman and Mattord, *Principles of Information Security*.
322. Tam and Jones, "Cyber-Risk Assessment."