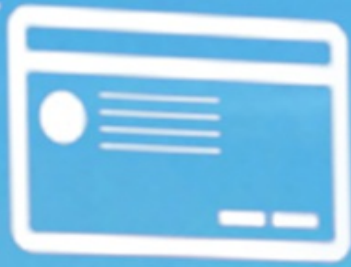


Second Edition

73%



INTRUSION DETECTED ...



Maritime Cybersecurity

A Guide for Leaders and Managers



Gary C. Kessler & Steven D. Shepard

Maritime Cybersecurity
A Guide for Leaders and Managers
Second Edition
Gary C. Kessler
Steven D. Shepard

Maritime Cybersecurity: A Guide for Leaders and Managers

Gary C. Kessler

Steven D. Shepard

Copyright © 2020, 2022 by Gary C. Kessler and Steven D. Shepard

Published in February 2022

9798412526034

Kessler, Gary C., 1953—

Shepard, Steven D., 1954—

Maritime Cybersecurity: A Guide for Leaders and Managers/

Gary C. Kessler

Steven D. Shepard

9798412526034

1. cybersecurity. 2. maritime transportation system. 3. security. 4. port cybersecurity. 5. ship cybersecurity. 6. autonomous ships 7. information technology 8. information security. 9. navigation systems

Dedications

Gary dedicates this book to the memory of his father, Bernard Kessler, “who frequently had more faith in me than I had in myself”; to his wife, Gayle, who is ever-supportive even while she shakes her head (and smiles); and to his grandchildren, Isabella, Louisa, Cohen, and Simon, who are the future.

He also dedicates this book to his colleagues and students in this emerging field around the world that he has met and with whom he has collaborated in the last five years.

Steve dedicates this book to his wife, Sabine, and to his grandchildren, Ayla, Maya, Jaxon, and Arya. Thank you for the joy you bring.

He also dedicates it to his co-author and long-time friend, dive partner, and co-conspirator, Gary Kessler. Thanks for all the fish.

Note to Readers

To keep the price of the book reasonable, we opted to publish it in black and white. Purchasers of the book can download color, full-sized versions of the images; to access the file that contains the illustrations, point your mobile phone's camera at the QR code shown below, or visit

https://www.garykessler.net/MaritimeCybersecurityBook/MaritimeCyberSecurityBook_2e_figures.zip.



In addition, to cut down on the page count (and, therefore, the price of the book), all references, as well as new papers and articles, can be found at [https://www.garykessler.net /MaritimeCybersecurityBook/#refs](https://www.garykessler.net/MaritimeCybersecurityBook/#refs) or by using the QR code below.



Table of Contents

[Dedications](#)

[Note to Readers](#)

[Preface](#)

[Chapter 1: The Maritime Transportation System](#)

[Chapter 2: Cybersecurity Basics](#)

[Chapter 3: Case Studies—Cyberattacks on the Maritime Sector](#)

[Chapter 4: Ports and Cybersecurity](#)

[Chapter 5: Shipboard Networks and Communications Systems](#)

[Chapter 6: Navigation Systems](#)

[Chapter 7: Operational Technology and Autonomous Systems](#)

[Chapter 8: Strategies for Maritime Cyberdefense](#)

[Chapter 9: Concluding Thoughts](#)

[Abbreviations and Acronyms](#)

[Acknowledgements](#)

[Figure and Table Credits](#)

[Gary C. Kessler](#)

[Steven D. Shepard](#)

[Index](#)

Preface

It was a dark and stormy night^[1]. Imagine that the following communication takes place between a fictitious cargo ship and the Vessel Traffic Service (VTS) at a fictitious port:^[2]

“VTS Port Neptune, VTS Port Neptune, this is motor vessel LADY P.”

“VTS Port Neptune, go ahead, LADY P.”

“Port, we are approximately three miles from the farewell buoy and are experiencing IT systems problems onboard. We have several status alarms sounding without cause, and AIS and radar show targets in our path, although we see no other vessels in our area. We are requesting transit to the cargo berth and will fix these problems at the pier.”

After a few moments, the Port responds:

“LADY P, the Captain of the Port deems your vessel unseaworthy at this time and you are denied entry. A cyber response team will be dispatched to assist your vessel.”

The Impact

What just happened? Why was this vessel denied entry into a commercial port, when the problem appears to be with its onboard instruments? And what is this *cyber response team*?

The answer, of course, is far more complex than that. LADY P was denied entry to the port because of a concern that the vessel might be the victim of a cyberattack. And depending on the nature of the ‘digital infection’ that appears to be affecting the vessel’s ability to safely navigate, there is a very real concern that, once berthed, the infection could spread to landside systems, which would pose a far greater threat than an attack limited to a single vessel.

According to a 2019 cyber risk survey, 79% of respondents ranked cyber risk among the top five threats to their organizations, up from 62% in 2017. Even more sobering is the number of organizations expressing zero confidence in their ability to understand and assess a cyber risk: that number rose from 12% to 19% in the same timeframe, and from 15% to 22% for their ability to properly respond to and recover from a cyber event. And couple this with reports that cyberattacks on maritime operational technology increased 900% between 2017 and 2020.

All too often, cybersecurity is relegated to the purview of the Information Technology (IT) Department. Ironically, though, while IT professionals play a crucial role in cyberdefense, in many ways they represent the *last* line of defense against a would-be cyberattacker and are not necessarily trained in risk management processes.

Let’s look at a different scenario, one in which a vessel, infected with malware from a cyberattack, is allowed to enter a port and tie up at a cargo berth. Once the infected ship has breached the walls of the port’s digital castle, as it were, it becomes a *de facto* part of the port’s network. And once the vessel’s network connects to that of the port, whatever was hiding in the vessel’s telecommunications and IT infrastructure can now make its way into the port’s network. Bad things start to happen: calls go out to IT; and while they may be able to limit the reach of the infection, the damage is done. And it doesn’t stop there: the malware can also make its way to other vessels at the port, as well as the trucking, railroad, and aviation carriers that service the multimodal port.

The scenario that we’ve just described could happen to any port, anywhere in the world. An attacker manages to introduce malware into a port’s information infrastructure by jumping across the interface between the ship’s and the port’s IT environments. This could happen because of something as simple as a crew member’s infected mobile phone connecting to the port’s Wi-Fi. Furthermore, neither the ship nor the port were necessarily specifically targeted, but were subject to an opportunistic cyberattack.

The malware could do something overt, like a ransomware or extortion attack, or it could do something much more insidious, such as exposing large volumes of sensitive customer data to the outside world. When that happens, trust and credibility disappear. At this point, the organization doesn’t have an IT problem—it has a potentially *existential* problem, because this intrusion creates damage that goes far beyond the IT organization: It extends deep into the company’s nervous system. The CEO must explain to shareholders, the board of directors, and regulatory agencies why this happened and how it will be prevented from recurring. The Chief Marketing Officer has a messaging nightmare to contend with, along with the laborious and complex task of trying to restore customer and marketplace trust. The Chief Operating Officer must create and implement a new set of operating protocols to deal with the issue. The Chief Financial Officer must respond to the economic blowback that inevitably results as customers, fearful of being compromised, go elsewhere with their shipments, leading to severe revenue shortfalls. The Chief Strategy Officer has the unenviable task of drafting long-term plans to coordinate the efforts of all parts of the

business, so that in the event of another attack – something that experienced businesses deem a matter of ‘when,’ not ‘if’—a plan will be in place to thwart it. And the sales organization faces the Herculean task of selling to customers with which the bonds of credibility and trust have been strained.

All of this from a seemingly benign decision to allow a vessel with an onboard cybersecurity problem to enter the port.

Historically, a ship with a cyber problem might have been assigned an escort, shut down, and towed into port, because any disruption of normal port operations has a noticeable downstream ripple effect. If the vessel was to be denied entry, there would be significant tangible and intangible costs associated with:

- Passengers intent on embarking and disembarking, as well as the impact to associated land transportation
- Cargo to be unloaded and offloaded, and the impacts of delay on the associated supply chains
- The disruption to the schedule of the port and the cost of an unused dock, idle stevedores, and delays to other ships
- The impact to this vessel’s schedule arriving at and leaving from this port, and arriving at the next port
- The effect on ground and air carriers awaiting cargo from this vessel
- The impact to passengers and/or owners of the cargo, as well as possible cargo spoliation

As cyber events on vessels become more common, ports and shipping lines, as well as the ships’ masters, must find better ways to resolve these challenges. In February 2019, a vessel en route to the Port of New York and New Jersey reported a cyber incident that was affecting its shipboard systems. The vessel was ordered to stay outside of the sea buoy. A U.S. Coast Guard (USCG) cyber team worked with the vessel and confirmed that all cyber effects were isolated to the ship. Once they were assured that the handling of the vessel and the control systems were not at risk, the vessel received permission to dock from the Captain of the Port (COTP). Today, USCG and maritime authorities around the world have established a growing number of Cyber Protection Teams (CPTs) with a mission to respond and assist to these types of events.

The problem of cyber activity goes well beyond ships at sea. A 2018 malware incident caused a ship’s electronic chart display and information system (ECDIS) to malfunction while it was docked. 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.

Why We Wrote This Book

A common but mistaken belief at the leadership level of many organizations, both within the maritime industry and beyond, is that the responsibility for protecting information assets lies within the technology ranks. Cybersecurity—or, arguably more properly, *information security*—is not merely, or even primarily, the responsibility of the IT department. Everyone who comes in contact with information in any form has the responsibility to protect it and, further, to recognize when it is under attack—and take whatever action is required to defend it, including reporting suspected attacks to the appropriate defensive agencies within the organization. Ultimately, it is the responsibility of a designated Chief Information Security Officer (CISO) to manage the cybersecurity posture of an organization. The CISO should be someone who understands the business risk elements of cybersecurity, not simply an elevated IT manager. That individual should champion a posture that includes a sense of urgency and awareness around cyberthreats at every level of the organization.

It is also important to recognize that IT and cybersecurity professionals have different—albeit often overlapping—skill sets. IT professionals keep networks running and resilient, maintain software and operating systems, and provide services and applications to the users; cybersecurity professionals defend these assets.

Where to From Here

The target audience of this book is the maritime manager, executive, or thought leader who understands their business and the maritime transportation system, but is not as familiar with issues and challenges related to cybersecurity. Our goal, reflected in the book’s structural flow, is to help prepare managers to be active leaders preparing maritime domain cyberdefenses. We assume that the reader knows their profession, knowledge that will help to provide the insight into how cyber affects their job role and organization.

Chapter 1 (The Maritime Transportation System, or MTS) provides a broad, high level overview of the MTS, the various elements within it that must be secured, and the size and scope of the challenge. Chapter 2 (Cybersecurity Basics) offers terms, concepts, and the vocabulary required to understand the articles that one reads and the meetings that one attends that discuss cybersecurity.

The next five chapters describe actual cyber incidents in various domains of the MTS and their impact on maritime operations. Chapters 3-5 address cyberattacks on shipping lines and other maritime companies, ports, and shipboard networks, respectively. Chapter 6 (Navigation Systems) discusses issues relating to global navigation satellite systems and Automatic Identification System (AIS) spoofing and jamming, while Chapter 7 (Operational Technology and Autonomous Systems) presents cyber-related issues and the ever-increasing challenge of remote control, semi-autonomous, and fully-autonomous systems finding their way into the MTS.

Chapter 8 (Strategies for Maritime Cyberdefense) discusses practices that address cybersecurity operations in the MTS, including risk mitigation, training, the very real need for a framework of policies and procedures, and the development and implementation of a robust cybersecurity strategy. Chapter 9 offers final conclusions and a summary.

It is impossible to write a book about a fast moving field such as this that remains up-to-date. And, indeed, many things have happened since the publication of the first edition that prompted us to write this update, including the release of the U.S. National Maritime Cybersecurity Plan, an increased number of ransomware and other cyberattacks directly targeting maritime stakeholders, a dramatic escalation in attacks on maritime navigation systems, disruptions in the global supply chain as evidenced by the blockage of the Suez Canal by EVER GIVEN and backups at the Ports of Long Beach and Los Angeles, and growth in operational technology, automation, and autonomy in maritime facilities—to name but a few.

To ensure currency and relevance, the book has a companion website at <https://www.garykessler.net/MaritimeCybersecurityBook> that points to a number of websites where current information and other active content can be found. We hope that the information presented in this book and the contents on the website will add to the resources that readers use to stay informed about this major threat to the maritime industry.

Gary C. Kessler *Steven D. Shepard*
Ormond Beach, FL *Williston, VT*

February 2022

Chapter 1: The Maritime Transportation System

Introduction

We recognize that many readers of this book have already spent years working in some segment of the maritime transportation system (MTS). While some of you might have deep familiarity with one or two segments within the MTS, your familiarity with the others, all of which are equally critical to the smooth operation of this critical infrastructure, may not be as complete. Other readers may have significant experience with supply chain management, large system operations, or physical or cybersecurity, but may be new to the maritime environment.

This chapter provides an overview of the MTS and presents a basis for understanding the segments that comprise it. Once we have established a baseline understanding of the many moving parts of the maritime transportation environment, we will discuss the cyber landscape of the MTS.

What We Are Trying to Secure

The maritime transportation system comprises ships, shipping lines, ports, passenger terminals, manufacturers, cargo facilities, intermodal partners, and all of the users of these facilities. Every element represents a potential vulnerability to a cyberattack—a potential weak point—and, therefore, a vector that can infect other elements within the MTS. The components that we tend to associate most with maritime are ships and ports. There are expected to be more than 70,000 merchant vessels on the water by 2023, operating in and out of approximately 4,800 ports in 200 countries. Merchant vessels, like airplanes and other forms of transportation, don't make money when they sit idle, so these ships are in constant motion (Figure 1.1).

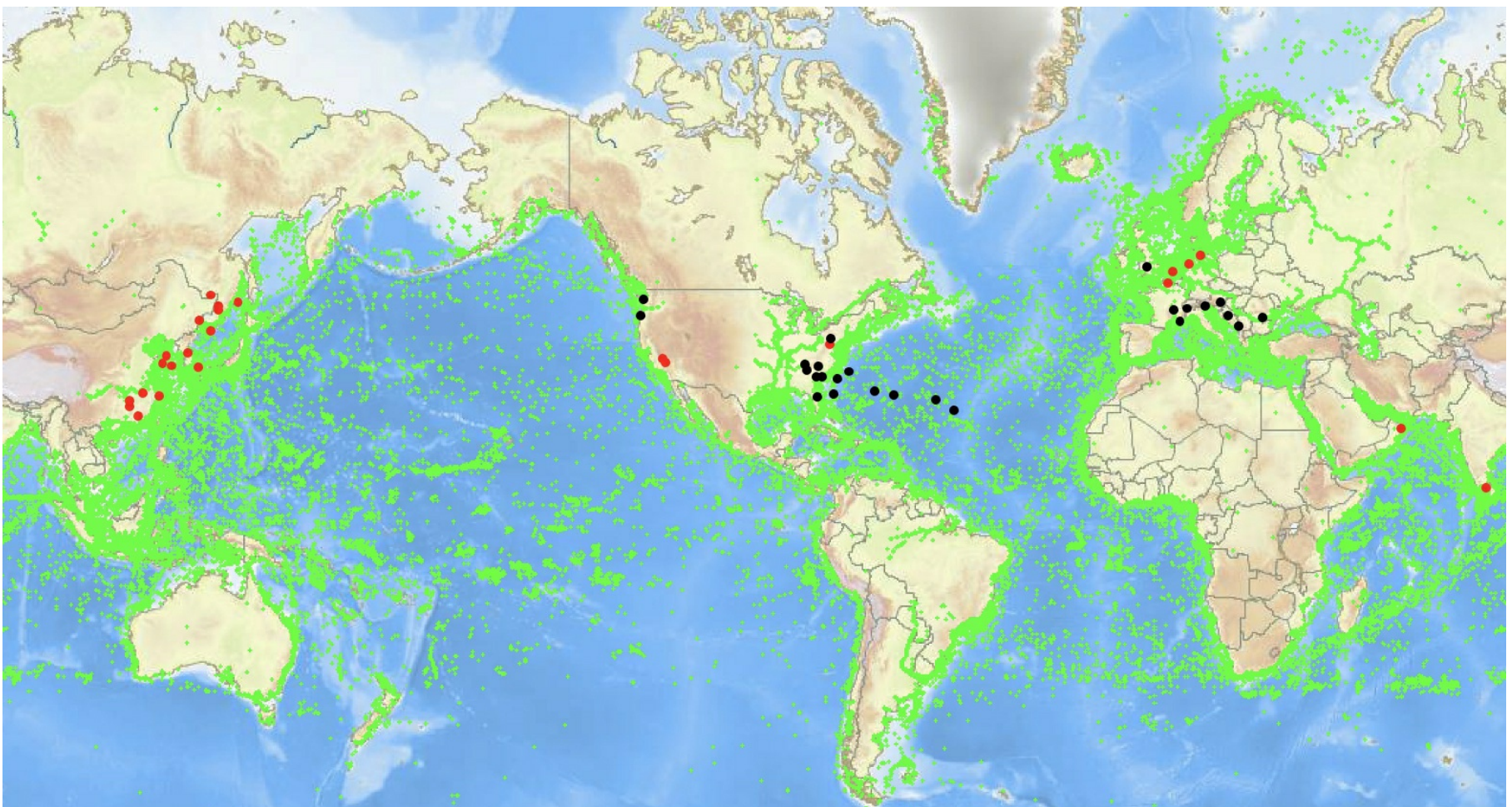


Figure 1.1. Ship positions worldwide, as reported from the Shipfinder website (26 April 2020), plus the 50 busiest cargo (red dots) and passenger (black dots) ports.

Maritime represents an integral part of the Transportation Systems Sector, one of the 16 critical infrastructures defined by the U.S. Cybersecurity and Infrastructure Security Agency (CISA). The transportation sector itself comprises maritime, aviation, trucking, railroads, and other forms of ground transportation. Transportation, of course, is what moves people and cargo from a point of origin to a destination. As such, all modes of transportation interact as cargo and passengers move between ships, inland waterways, railroad cars, trucks, and airplanes. These intermodal connections provide additional vectors for cyber infection between elements of the broader transportation sector.

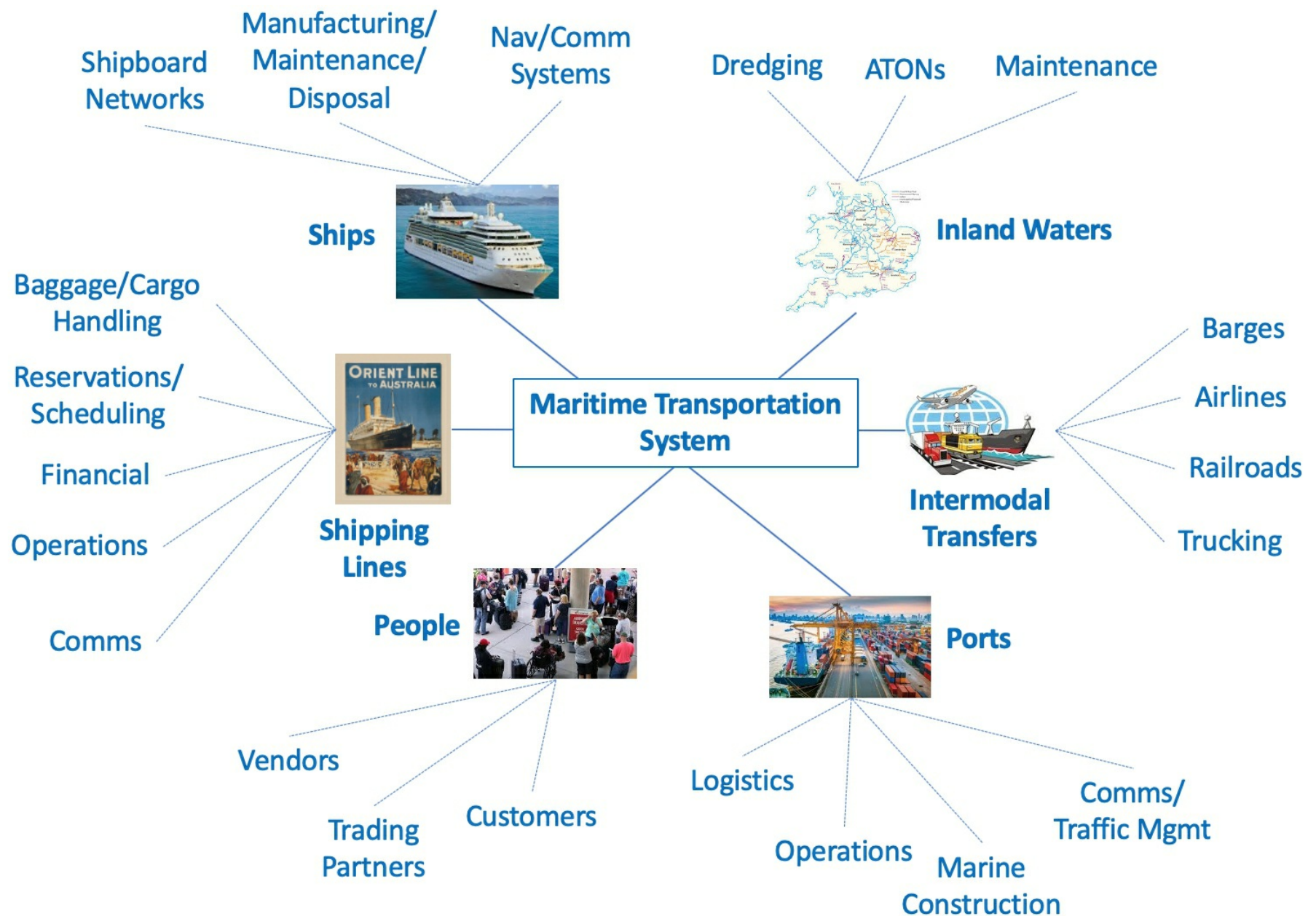


Figure 1.2. The MTS system of systems.

MTS: A System of Systems

The MTS is not monolithic, but rather a system of systems. In one model, the MTS comprises six interconnected systems: ships, shipping lines, ports, people, inland waterways, and intermodal transfers (Figure 1.2); in turn, each of these systems has its own sub-systems. The systems are unique and independent of each other, yet co-dependent and inextricably intertwined. The life of a ship, for example, intersects with the life of a port and is only a part of the life of a shipping line. People and cargo intersect with a ship's voyage and transit through ports, intermodal transfers, and inland waterways. The cybersecurity threats to the MTS are similar to threats everywhere else in the information space, but are unique to our industry and way of life.

- The *Ships* subsystem includes aspects in the lifecycle of a vessel, from manufacturing, to maintenance, to operations, to disposal. From a cyber perspective, ships are floating networks that need to interconnect multiple operational networks, passenger/entertainment networks, and navigation system networks, as well as other vessel-specific networks.
- The *Ports* subsystem includes the construction and maintenance of the port, logistics within the port, vessel traffic management, interactions among the various intermodal carriers that enter and leave the port carrying cargo, and all aspects of daily port operations. All ports are unique and have a different combination of ownership and management, a different mix of civilian and military vessels and operations, the interconnection of IT systems by port operators and tenants, personnel management, intermodal connections, volume of traffic, cargo, passengers, and more. Intellectual property (IP) theft related to port operations and construction can yield very valuable information to competitors and adversaries, alike.
- The *People* subsystem includes the entire supply chain, trading partners, vendors, and customers. People are often the largest threat to security, both physical and cyber. They are our passengers, our workers, our adversaries, our clients—our colleagues. We need to vet the people that are engaged in any way with the MTS, obviously at different levels. Cyberattacks on the personnel or passport control systems can render ordinary security checks worthless, not to mention the threat to the enormous amount of personally identifiable information (PII) and financial information in the personnel and passenger databases.

- The *Shipping Lines* subsystem comprises the operation and management of the companies that own the ships, and includes handling of passengers and cargo, reservation and scheduling systems, finances, operations, and communications. A shipping line is a business just like any other business, one that just happens to own and operate ships. They have every potential security vulnerability that any other business does, from finance and logistics to communications and cargo/passenger management. Like any business, there is a significant amount of third-party software and systems employed by the shipping lines, and while this can be an advantage from a reduced complexity perspective, it also means that they're not in total control of many of their own systems.
- The *Inland Waters* subsystem includes the inland waterway system, associated aids to navigation, and dredging and maintenance of the waterways. Attacks on vessels operating in inland waters can cause tremendous havoc in narrow waterways such as Kill Van Kull, the Suez Canal, or the Panama Canal.
- The *Intermodal Transfers* subsystem describes how the maritime sector interfaces with other transportation modalities, including the inland barge system, railroads, trucking, and aviation. This is where the MTS touches everything else. Even if a port, ship, and shipping line have the best possible security, they are vulnerable to an oblique attack via a trading partner. As an example, if a Bad Actor breaks into a shipping company's trading partner and prepares a bogus order that results in a truck arriving at a port with a bill of lading, the port will allow the truck to pick up a shipping container.

All of these systems must also contend with new generations of information and communications technologies, automation, operational technology, the Internet of Things (IoT), artificial intelligence, smart devices, machine learning, unmanned systems, and more. Each maritime stakeholder must integrate these new elements into their own operations, even as they remain compatible with their maritime and other business partners.

Size, Scope, and Users of the MTS

While most ordinary citizens do not necessarily appreciate this fact, any country with a coastline and a port can consider themselves to be a maritime nation. Furthermore, most inland countries are dependent upon the MTS for much of their goods. Approximately 90% of the world's cargo, after all, travels by ship. There are approximately 90,000 ships (including coastal vessels) engaged in the transport of cargo and passengers; these ships have an asset value of about \$2 trillion and carry more than \$19 trillion of cargo annually.

The MTS is a significant economic driver for any coastal nation. It is, as noted earlier, the largest import/export transportation modality globally. In the United States (U.S.), as an example, 40% of all imports come through the Ports of Los Angeles and Long Beach alone. Furthermore, the maritime industry contributes \$5 trillion—approximately 25%—to the U.S. annual gross domestic product (GDP) and supports 30 million jobs, representing nearly 20% of the nation's workforce.

The U.S. MTS includes 25,000 miles of navigable channels, 95,000 miles of shoreline, 361 commercial ports, 50,000 federal and innumerable private aids to navigation (ATONs), 20,000 bridges over water, more than 3,700 marine terminals, 200 ferry operations, and 238 locks at 192 locations. The MTS user community also includes hundreds of thousands of small charter fishing, sightseeing, work, liveaboard, and dive boats, as well as more than 12 million recreational boats.

A nation's maritime waterways are shared among many user communities. We have already mentioned the ports and commercial cargo and passenger ships, but there is also an entire system of coastal and ocean-based weather, navigation, and communications stations and buoys. Near coastal and inland waters are also home to:

- Military, public safety, and law enforcement vessels;
- Work boats, dredge boats, survey vessels, buoy tenders, and other vessels engaged in waterway and ATON maintenance;
- Commercial fishing vessels;
- Personal power boats and sailing vessels; and
- Drilling platforms, moorings, wind turbines, and other fixed-location offshore facilities.

Cyberattack Vectors in the MTS

It should be clear that the MTS environment comprises countless moving parts, each of which plays a critical role in maritime transportation safety and operations. We cannot emphasize enough the fact that every one of those moving

parts represents a potential cyberattack vector or victim, which is why it is so critical to have a holistic view of the entire MTS system, not just the segment that your particular job title lends itself to.

There are a vast number of cyberattack vectors through and within the maritime environment. For example:

- *Vessel operations:* Modern ships are floating computer and data communications networks, including the operational networks controlling ship systems, networks connecting security and cargo management systems, bridge systems for navigation and communication, entertainment networks on passenger vessels, and weapons control networks on warships. As we will see, navigation and communication systems are also possible vectors for cyberattacks.
- *Shipping line operations:* Both cargo and passenger shipping lines have complex outward facing networks as well as many internal networks. The public Internet, for example, typically hosts a company's open website and e-mail server, as well as customer and partner portals, electronic commerce (e-commerce) capability, reservation systems, ship and cargo tracking systems, sales and marketing information, and more. Internal networks manage vessel communication, passenger and cargo tracking, personnel management, payroll, logistic and supply management, financial management, baggage and cargo handling, customer/partner relations, maintenance scheduling, legal compliance, route management, and more. Each of these functions can be a target and a pathway for a cyberattack.
- *Port operations:* Ports also have their own Web presence, sales and marketing systems, vessel and cargo tracking systems, and portals for customers, tenants, and supply chain partners. Port physical security systems, such as cameras and sensors, are also generally managed by network controllers. Communications are essential between the terminal headquarters, vessel traffic management, ships entering and leaving the port, port tenants, financial partners, legal authorities and customs, and shipping lines. Like any well-run business, ports also have personnel management and financial systems, as well as links to customs and immigration for cargo, passengers, and crew. Additionally, ports have their own logistics and inventory systems because they, too, are customers to their own set of equipment suppliers.
- *Cargo and shipping:* Cargo-related networks provide connection to customs, business partners, and the owners of the cargo that is temporarily stored at the port. Cargo-related operations also include many industrial control and automation systems that manage movement of cargo around the port and the cranes used for cargo onloading and offloading. Cargo security is also controlled by computers, as well as the handoff of cargo to and from intermodal carriers, with necessary linkages to rail, truck, and air carriers.
- *Manufacturing:* Manufacturers have the same information assets as the shipping lines and ports in terms of public websites for marketing, recruitment, and general information, as well as a customer portal for sales, order tracking, and payments, and internal systems for personnel management and payroll. Supply chain management is incredibly important to manufacturers to keep their production lines moving, which includes their ability to move money as well as goods. Intellectual property theft is a significant existential threat to manufacturers, as the theft of proprietary information by rival companies is often enabled by the Internet. An adversary can cause a number of disruptions in the highly organized, complex choreography of a ship's manufacturing process by modifying the work schedule so that essential skilled workers are not available when needed, changing part ordering and delivery schedules so that needed parts are not in the right place at the right time, or altering manufacturing blueprints so that one block of a ship does not fit properly with another. Such disruptions can result in huge financial losses and project delays. Trojan horse flaws can also be introduced, where equipment works as it is designed but with an exploitable flaw that can be accessed by a Bad Actor at a later time.
- *Vessel traffic control (VTC):* Managing the flow of vessels, particularly in a busy port or a narrow body of water, requires reliable radio communications; positioning, navigation, and timing (PNT) systems, such as the Global Positioning System (GPS); situational awareness networks, such as AIS; up-to-date charts and notices to mariners; and other functions that maintain safe and efficient movement of ships, cargo, and people. Each of these systems provides a potential vector for cyberattack in geographic areas that can tolerate a low margin of error. Couple this with the fact that while nearly all ports commingle military, commercial, and/or recreational vessels in the same waterways, these boats and ships are not generally under control of the VTC system.

- *Remote control and autonomy:* Unmanned and autonomous vessels, vehicles, and other port operations are emerging throughout the world due to a shortage of personnel, safety concerns, economic imperatives, and other factors. These systems range from remote controlled to fully autonomous ships, tugs, docking facilities, drones, trucks, and cranes. Unless properly secured, each of these can be, at best, manipulated to become non-functional or, at worst, turned into a physical weapon. Imagine the potential economic and environmental damage that could occur if a vessel loaded with liquefied natural gas (LNG), for example, were to enter a port facility at high speed, under the control of a Bad Actor, and ram another vessel or run itself aground.

The snapshot above is only meant to provide some insight into the complexity and number of systems required to keep the MTS working. It is also a non-exhaustive list of cyber targets. Keep in mind that a vulnerable system that can be exploited may not be an attacker's actual target; a system or network, once compromised, can serve as a jumping-off point to gain entry to other, more 'attractive' targets, such as a system at a trading partner, supplier, or vendor. Thus, a good cyberdefense posture protects not just the organization's own systems, but all of the systems with which that organization's data comes in contact. Remember, attackers don't want your computers or networks; they want your information or to disrupt the flow of information.

And *that* is the very definition of a partner in the context of cybersecurity. A partner is any entity that affects, in any way, the chain of custody of your data. If your data never leaves your corporate intranet, then a partner is any entity that has access to your intranet. If you send information over a public network, then a partner is any entity that has the necessary security credentials to access your data or can interfere in any way with the movement of your data.

There are many rules, regulations, and laws that guide the maritime industry, not to mention policies specific to different nations, ports, and shipping lines. Although several organizations publish guidance about handling cybersecurity (more on that in Chapter 8), no single organization is responsible for the IT systems that keep the MTS moving. Furthermore, most organizations do not fully own (or operate) their IT infrastructure. Consider, as examples:

- An organization's website is often hosted by a cloud service or other provider. Reservation, ticketing, and payment systems are often managed by a third-party e-commerce host, and always include some way to exchange funds with a financial institution.
- The corporate network for a port, shipping line, manufacturer, or supplier is generally a private network with its own hosted IT infrastructure. Virtual private networks (VPNs) often provide access to the internal network via the public Internet.
- Civilian ships generally have multiple onboard networks. The ship's internal network controls shipboard functions, such as propulsion, power, status monitoring, and ballast. Another private network provides communications with the corporate network. The ship is also likely connected to the Internet for crew, passenger, and entertainment communications, as well as corporate communications—and provides the pathway for the private networks to communicate with their land-based counterparts. GPS, AIS, and communication with VTC also use public radio channels.
- Port operations use a combination of private networks for internal communication, public networks for navigation and communication, and, likely, networks for inter-modal communications, ship supplies, and cargo and passenger management. Ports also have a variety of methods with which to communicate with ships.

Conclusion and Summary

The purpose of this chapter is to demonstrate the size and value of the MTS to the economy and, indeed, our very way of life, as well as the enormity and complexity of its cyber structure. Alas, the MTS also represents a huge cyberthreat surface, given that every system within it represents a potential attack vector. And, keep in mind that every person with access to corporate data represents a potential threat, intentional or otherwise.

Chapter 2 will discuss cybersecurity terms and concepts to put cyber vulnerabilities and attack methods in context.

Chapter 2: Cybersecurity Basics

Introduction

Friday, May 12th, 2017, was a Friday. The only newsworthy thing that happened that day was that Harry Potter author J.K. Rowling publicly asked her readers to refrain from buying a Harry Potter prequel that she wrote, a manuscript which had been stolen and was up for auction. That was the only thing of note that day, that is, until calls began to hit IT tech support agencies throughout the world, all with the same complaint—“my computer is locked up, and whoever did it wants money to unlock it. And if I don’t pay, they say, they’ll delete my files forever.”

This was a serious, coordinated ransomware attack, one of many techniques that cybercriminals can exploit to their advantage. According to Europol, 200,000 computers in 150 countries were affected by that ransomware campaign within 48 hours, most of them in India, Russia, Taiwan, and Ukraine. And the attack wasn’t limited to the personal computers of individuals. The U.K. National Health Service was hit hard by the attack, which affected 70,000 of their devices, including magnetic resonance imaging (MRI) machines, blood bank refrigerators, computers, and surgical theaters. Ambulances had to be diverted and hospital-based care had to be rescheduled.

The U.K.’s healthcare infrastructure wasn’t the only victim. Nissan had to close manufacturing facilities in the U.K. when it discovered that some of its systems were infected. Renault halted production to slow the spread of the ransomware. Telefónica in Spain, Deutsche Bahn, and FedEx were also affected.



Figure 2.1. Screen shot of WannaCry ransomware.

The attack and the software behind it were quite sophisticated, and while it has not been conclusively proven, most authorities point to North Korea as the source of the malware, a ransomware program called WannaCry. When it executed, WannaCry burrowed into computers and encrypted the data stored on them. A payload message was then displayed on the computer screen, informing the computer’s user that their files had been encrypted and would be released when a ransom of \$300 was paid in Bitcoin. The victim had three days to make the payment, after which the price climbed to \$600. If they didn’t pay after seven days, the data was irretrievably lost (Figure 2.1).

Luckily, WannaCry was stopped after a few days by cybersecurity researchers, but not before serious damage was done. According to Cyence, a firm that models cyber risk scenarios, the economic impact of the WannaCry attack

was anywhere from hundreds of millions to billions of dollars.

What this scenario illustrates is that while Internet connectivity is a modern-day blessing, it can also be a modern-day curse.

Anyone today who reads a newspaper, attends a conference, or talks with colleagues is aware that cybersecurity is a threat with which all organizations, agencies, entities, or holders of information must contend. But cybersecurity is not monolithic; it is a suite of problems rather than a single threat and, therefore, requires multiple defensive strategies. And while ransomware is pretty sensational and gets a lot of newsprint, it is not the most common cybersecurity problem. This chapter provides a brief introduction to terms and concepts that will help you understand what it means to protect information, define different types of cyberattacks, and identify the nature of Bad Actors in cyberspace.

Characteristics of Information

Prior to the adoption of terms such as *cybersecurity* and *cyberspace security*, the practice was called *information security* or *information assurance*, titles that ensured a focus on the information itself rather than on the containers and communication pathways (although, to be fair, prior to that it was called *computer security* and *network security*). While we store most—but not all—of our information on computers, exchange information via networks, and deal with attacks coming from anywhere in the world via the Internet, the bottom line is that today, we have to look more at the content that we want to protect rather than at the ways in which we store and transport it.

So, what is it about information that are we trying to protect? Common parlance in the discipline is to describe the characteristics of information in terms of the *confidentiality-integrity-availability (CIA) triad*:

- *Confidentiality*: Protecting information from unauthorized access or disclosure; keeping secrets safe.
- *Integrity*: Information being free from inadvertent or deliberate manipulation.
- *Availability*: Information being accessible when needed.

Security expert Donn Parker added another three characteristics that, when added to the CIA triad above, yields the so-called *Parkerian Hexad*:

- *Possession*: Custody of data by the authorized user.
- *Authenticity (aka authentication)*: The ability to prove the identity of the sender or owner of information, and that the information is real.
- *Utility*: The usefulness of data to the user (e.g., there is no utility in possessing encrypted data without a decryption key or receiving a message to do something after the date when the action is required).

Types of Cyber Vulnerabilities

This is one of the longest single sections in this book. It is meant as a reference that defines nearly 30 different types of cyber vulnerabilities. The section begins by describing social engineering, malicious software, phishing, denial-of-service attacks, ransomware, and several other common forms of cyber vulnerability that appear in the media on an almost daily basis. The latter part of this section briefly describes another two dozen cyber vulnerabilities about which the reader should be aware. The purpose here is to provide a context for what these terms mean in the realm of cybersecurity and to demonstrate the countless types of cyberattacks that are possible. Alas, it is far from an exhaustive list.

Social Engineering and Malicious Software

Social engineering is a form of psychological manipulation where a Bad Actor persuades a Good Actor to do something that is not in the Good Actor's best interest—including actions that run contrary to the law, policy, or regulation. Social engineering attacks can be very sophisticated and even trained individuals can fall victim to a well-organized social engineering campaign. This is the basis for any number of frauds; in cyberspace, social engineering is a primary vector for convincing people to download malicious software, open an attachment to an e-mail, go to dangerous websites, and otherwise violate good cyberhygiene practices.

A cyberattack via social engineering does not require a computer or even a cyber vector. Imagine a scenario where a well-dressed young woman enters corporate headquarters and goes to the reception desk with a coffee-stained resume. "Can you please help me?," the panicked young woman says. "I'm here for a job interview that starts in 15 minutes, and I spilled coffee on my resume. I have a copy on my thumb drive. Can you print a new copy for me?"

What receptionist doesn't remember their first job? Of course, they'll help. And on the thumb drive is the resume file, so all is good. On the thumb drive is also other nasty software that we'll describe below that is now on the receptionist's computer and, most likely, looking for ways to move around the corporate network. The young woman profusely thanks the receptionist and quietly exits by the back door.

Malicious software—aka *malware*—generally refers to programs and applications that intentionally disrupt the operation of computers and communications systems, including user systems, servers, local networks, and the Internet. Malware targets a variety of the CIA characteristics of information described above. Nearly all malware gets into a computer or network when a user opens an attached file in an e-mail, downloads an infected file from an Internet site, or otherwise responds to directions provided in a message from an “unknown” user.

Most people are familiar with the terms *computer virus*, *worm*, and *Trojan horse*. A virus is malware that is activated by the user, often by opening an e-mail file attachment. Once active, a virus can do almost anything on a computer system or mobile device, such as slowly deleting data, degrading the system's performance, or making the computer part of a zombie network used to attack other systems.

Spyware is a type of virus that exfiltrates data by collecting keystrokes, contents of the system clipboard, screenshots, user login credentials, and other information that can be uploaded to an attacker's site.

Worms are malware that can replicate and spread to other systems, usually by forwarding themselves to all addresses found in the infected system's address book or advancing via open network shares. Like viruses, worms can do just about anything to the host computer once they are active; even without a malicious payload, they can degrade the performance of a computer. Worms are now the most common way in which malware makes its way around the Internet, and worm-based malware can infect hundreds of thousands of computers within minutes or hours—as we saw with the WannaCry scenario described earlier.

Trojans, or *Trojan horses*, are programs that are intended to do one thing but that also contain additional, malicious functionality. Once invoked, these programs allow a Bad Actor to control every aspect of the infected system. Remote Access Trojans and other Trojan horse programs can be found in e-mail attachments or at software download sites, but are also distributed at some gaming, music sharing, and pornography websites, where users are told to download special viewing software to access the files. An example is CoinTicker, a MacOS X application that monitors the current price of Bitcoin and other cryptocurrencies, but also installs malicious backdoor programs that allow an attacker to gain access to a user's cryptocurrency wallet. The malware remains on the system even after the main program is deleted. While most malware targets Windows systems, this example was specifically used to demonstrate that Linux and MacOS computers are not immune to malicious software and hacking.

Viruses and Trojans are pervasive on mobile devices, particularly those that use the Android operating system and the open app store. Mobile devices are an especially attractive target for attackers because of the huge amount of personal information that they contain, including e-mail, text messages, photographs, financial and health information, login credentials for work networks and dozens of apps, and more. Information-stealing software is as likely to target mobile devices as it is personal computers.

Phishing and Watering Hole Attacks

Phishing is a form of social engineering in which an individual receives an e-mail message from what appears to be a legitimate source, that asks the recipient for some form of PII, protected health information (PHI), or network-sensitive credentials. Phishing is a form of fraud and uses trickery, manipulation, and, in some cases, intimidation for its success. Themes of phishing messages might include:

- Notification of a compromise of, or questionable charge to, a credit card or bank account
- Notification of winning the Irish Sweepstakes, a lottery, a gift card, or other award
- An unsolicited job offer
- A request for information in order to continue to receive benefits (e.g., Social Security), keep an account open, receive a tax credit, or repair/validate a password database
- A demand for payment to settle a tax judgment from the Internal Revenue Service (IRS) or pay a fine to avoid being arrested by the Federal Bureau of Investigation (FBI)

With phishing, the attacker's goals are to perpetrate financial fraud or identity theft, but these same schemes can also be used for intellectual property theft, access to sensitive information, or intelligence gathering.

Simple phishing attacks usually involve an e-mail directing the recipient to a bogus, but legitimate-looking, website. A *spearphishing* attack specifically targets individuals with some form of mutual bond or common interest, such as financial officers, employees who attended a meeting or class together, crew members on a particular ship, etc. Spearphishing messages can be highly personalized and made to appear very convincing. *Whaling* is a variant of

spearphishing, in which messages are directed to senior executives and managers, board members, or other high-ranking, high-profile individuals within an organization.

In the world of sales, a place where salespeople strive to get meetings with the highest-ranking executives that they can, a commonly heard mantra is, “You will be handed off to the person you sound the most like.” In other words, if you sound like an executive, you will be allowed to speak with another executive. The same holds true in the world of cybersecurity: If a message sounds legitimate, and the content appears to be relevant to the recipient, then the chances that the message will be opened and acted upon are much higher and much more likely to cause damage.

Phishing is not limited to e-mail. *Voice phishing* (aka *vishing*) sends the bogus message, often in the form of a threat of imminent arrest by a law enforcement or governmental agency, using the voice network, usually employing a synthesized voice and robocalls. Similarly, *SMS phishing* (aka *smishing*) uses text messages as the vector for phishing. On mobile phones, the caller’s number is often spoofed so that the message appears to come from the same area code or country as the target.

A variant of phishing is a *watering hole attack*, a focused form of social engineering that attracts groups with a common interest. The attacker starts by gathering intelligence on the targeted victims to determine or otherwise observe what websites the group often frequents (e.g., does everyone go to the same sports or news site every morning?). If the attacker cannot find such a website, a sophisticated adversary might create such a site specifically to attract the targets to one place. The next step is for the attacker to insert malware into the watering hole site, which, over time, infects susceptible user systems. As more systems become 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 can be victimized by watering hole attacks because of users’ inherent—albeit often undeserved—trust in the security of websites.

Denial-of-Service Attacks, Botnets, and Zombies

Another threat to the availability of information is a *denial-of-service (DoS)* attack. DoS attacks generally succeed by using a resource exhaustion strategy in which the attacker uses a variety of methods to either consume all of the available bandwidth on a communications channel or all of the processing power at an Internet-based server. The first DoS attack on the Internet occurred in 1996 when Panix, one of the world’s oldest Internet Service Providers (ISPs), was flooded with so many simultaneous connection requests that its servers crashed, and it went offline for days.

Early DoS attacks had a single attack source and, therefore, could be tracked back and attributed to the originator. In a small twist, a *distributed denial-of-service (DDoS)* attack employs tens of thousands of computers that are compromised with a form of malware that puts them under control of a behind-the-scenes attacker. The compromised systems run the malware—called a *daemon*—in the background, unseen by the user, turning the computer into a *zombie*. The collection of zombie systems is called a *botnet* (robot network). When the attacker is ready to launch a DDoS attack on a victim, they send a message to the compromised systems within the botnet, directing them to simultaneously send their malicious payload to the victim site so that the combined bandwidth demands of all of the zombies exceeds the ability of the victim site to service all of the requests.

Two of the largest DDoS attacks to date occurred within days of each other in 2018, when victim sites were flooded with up to 1.7 terabits per second (Tbps) of traffic, totally shutting the sites down. DDoS attacks do not require the attacker to have any special access to the victim’s network to cause a disruption or total blockage. For that reason, DDoS attacks by an organized adversary are a real threat to any network operation. While there are DDoS attack mitigation methods, there is also a time lag between the start of an attack and the network’s ability to respond, making an effective response that much more difficult.

Ransomware

Ransomware is a form of malware that locks a user out of a computer or file system unless the user pays a ransom. Ransomware attacks, such as the WannaCry events described earlier, have been around since about 2012 and can be used to attack any type of computer, including mobile devices. They have also been one of the top forms of cyber malware since 2016.

Ransomware is generally distributed as a virus or a worm. It typically works by encrypting the system’s files to make the system inaccessible to the user, and then demands a ransom payment in order for the user to recover the decryption key. In most cases, the ransom demand requires payment of a certain amount of money within a few days, then doubles the amount for the next few days, and then expires; this gives users very little time to attempt to decrypt their machine (which generally will fail). Sometimes, the Bad Actor will publicly release a few of the files to encourage reluctant victims to pay the ransom. Payments are made by anonymous cryptocurrencies, such as

Bitcoin or Monero. In most cases, the decryption key is delivered to the victim upon payment, because ransomware is generally distributed by cybercriminals who just want the money; if word got out that the key was not provided upon payment of the ransom, future victims would not pay. Ironically, many forms of ransomware include a helpdesk so that the victim can learn how to create a cryptocurrency wallet and transfer funds; as suggested above, this is a moneymaking business for cybercriminals.

Ransomware is increasingly used to target health care, financial, and public sector sites around the world. More than 400 local and state municipalities, including law enforcement agencies at all levels, have been targeted in the U.S. alone since 2013; 22 cities in Texas, for example, were hit in a single attack over just a few days in 2019. The maritime industry has certainly not been immune, with regular ransomware campaigns targeting ports, shipping lines, and other MTS stakeholders since early 2020. A common thread of these attacks is that operations grind to a halt, employees lose Internet and e-mail access, departments have to resort to pen and paper, and records are lost.

Ransomware is more than a nuisance. The number of ransomware attacks, both targeted and non-targeted, is rising at a nearly exponential rate. Nearly 40% of victims pay the ransom. The ransom amounts demanded are also on the rise, with a more than 500% increase since 2019. While \$300 (per system) was a common ransomware demand in the 2017-18 era, the 2021 average ransom is more than \$500,000 and the largest ransomware demand from a single victim is \$50 million. Ironically, ransomware groups often break into cyberinsurance company databases to target companies that are insured, thus almost guaranteeing that the ransoms will be paid. Total costs of downtime and recovery, plus the impact on a company's reputation, can run well more than the ransom.

Advanced Persistent Threats (APTs)

An *advanced persistent threat* is a cyberattack that generally has three main characteristics. First, attackers use a broad array of tactics, techniques, and procedures (TTPs), employing commercial, open source, and even home-grown computer and network intrusion tools. The methodology is advanced, even if the individual tools are not. Second, these attacks target a specific organization or industry rather than taking a random, scattershot approach; they generally employ low-and-slow techniques to avoid detection. Their goal is long-term access rather than short-term disruption. The attack is somewhat relentless; when faced with a strong cyberdefense, the attackers keep trying, using different TTPs. Finally, APT operators act deliberately with intent to cause harm, generally being based on coordinated actions sponsored by nation-states or highly organized groups. Do not lose sight of the fact that APTs are well-planned and focused; APT campaigns are not generally mounted to cause short-term noticeable damage and system outages but, rather, long-term access to the compromised systems, exfiltration of data, and staying hidden.

The APT term was coined in 2010 after Google publicly acknowledged that they had been subjected to a highly persistent cyberattack by the Chinese People's Liberation Army (PLA) Unit 61398 during the latter half of 2009. Dubbed Operation Aurora, Google and reportedly dozens of other organizations (including Adobe Systems, Juniper Networks, Northrop Grumman, Symantec, and Yahoo!) were attacked, losing intellectual property and other proprietary information. This first APT exploited a vulnerability in the Internet Explorer browser that had been reported to Microsoft in September 2009 but had not yet been patched. As a result of this event, Google closed its Chinese operation.

APTs are insidious attacks, rarely showing signs of hostile activity in their early stages. They start with the attacker doing a thorough reconnaissance of the intended target's network and public servers. Any number of mechanisms might then be used to gain access to the network, from social engineering and phishing to the installation of malware and use of standard hacking tools. Once in, the intruder does not cause any noticeable damage; indeed, they use this opportunity to search the network, move laterally to other systems, escalate privilege for further exploitation, and maintain their presence while striving to remain invisible. Goals of an APT might be monetary gain, intellectual property theft, espionage, or other long-term objectives.

Zero-Day Exploits

All forms of malware, as well as system and network hacking, exploit vulnerabilities in software, either at the operating system or application level. As these vulnerabilities are discovered, software vendors fix them, generally by updating the software or distributing patches. The sheer volume of vulnerabilities, however, makes it impossible for them to all be fixed; in fact, it's impossible for all software flaws to even be detected. Based on severity, vendors prioritize which flaws get fixed immediately and which have to wait. Only the highest priority vulnerabilities get fixed during any given update cycle, meaning that some remain unaddressed for months or, in some cases, years.

The term *zero-day exploit* refers to an exploit of a vulnerability that was either unknown or unpatched before the attack on that vulnerability took place. There is no short-term response to a zero-day exploit because the victim has to first determine what is happening and, possibly, must contact the vendor for a fix. Operation Aurora, described

above, is a good example; this first APT started in mid-2009 by exploiting a previously unknown Internet Explorer vulnerability. Microsoft did not create a patch for the flaw for some weeks after its discovery.

Zero-day exploits have become weapons of cyberwar. Bad Actors specifically look for relatively minor vulnerabilities in software so that they can create and stockpile exploits. Perhaps the most public display of the weaponization of zero-day exploits is the set of cyberattack tools (reportedly developed by the National Security Agency (NSA) and Central Intelligence Agency (CIA)) released to WikiLeaks in 2017. The tools included zero-day exploits for all major operating systems, financial and banking applications, smart televisions and other IoT devices, and many types of routers. It was one of these leaked zero-day tools—called EternalBlue—that became the basis for the WannaCry ransomware attack described above (and, in more detail, in the next chapter).

- | | |
|---|---|
| <ul style="list-style-type: none"> • APT/organized attack • Business e-mail compromise (BEC) • Brute force attacks • Confidentiality breach • Counterfeit hardware • Cryptojacking • Data alteration/diddling • Data breach • Data leakage • Data theft • DoS/DDoS • E-mail scams • Eavesdropping • Host exploit • Ineffective disposal • Ineffective testing • Insider threat | <ul style="list-style-type: none"> • Malicious code (malware) • Man-in-the-middle • Password spraying • Phishing, spearphishing, SMSishing and vishing • Physical exploit • Proxyware • Ransomware • Reconnaissance • Salami attack • Session hijacking • Social engineering • Supply chain integrity • Unauthorized access • Unpatched systems • Watering hole attacks • Zero-day exploits |
|---|---|

Table 2.1. A non-exhaustive list of threats to information.

Other Types of Threats to Information

Table 2.1 provides a long list of additional threats to information in addition to those touched on above. This non-exhaustive list is not meant to overwhelm the reader, but to ward off any tendency toward complacency brought about by thinking that a firewall and anti-virus software provide adequate protection against attack.

The paragraphs below provide brief descriptions of these additional threats.

- *Business e-mail compromise (BEC)*: BEC is a specific form of cybercrime perpetrated by e-mail fraud. Fake invoices or other financial instruments coupled with carefully-selected e-mail recipients are a hallmark of this type of cyberattack.
- *Brute force attacks*: Password cracking by attempting every possible combination of characters, numbers, and symbols.
- *Confidentiality breach*: Loss of corporate or personal private information, with consequences including civil and/or criminal liability, loss of public/customer confidence, identity theft, access to supply chain partners, loss of sensitive or classified data, etc.
- *Counterfeit hardware*: Copycat hardware that appears to operate like the original but does not meet the required design specifications, such as processor chips and memory devices that might unexpectedly fail, operate at a slower speed than required, or utilize excessive power. Even cables can be problematic; the O.MG cable looks exactly like an Apple Lightning cable for charging an iPhone from a Universal Serial Bus (USB) source, but contains malicious hardware and firmware that allows an attacker to take control of the cable. If connected to a Mac computer, the attacker can upload malware and seize control of the device.
- *Cryptojacking*: Cryptocurrencies, such as Bitcoin, Ethereum, and Monero, secure their transactions in a

public list called a *blockchain*. Transactions are verified by *miners* who solve a cryptographic puzzle specific to a set of transactions, called a *block*. The first miner to validate a block of transactions is rewarded, usually with some amount of cryptocurrency; all other miners who solve the puzzle for that block get nothing. To avoid the real costs of possessing sufficient processing power and electricity required to be the first miner to solve the puzzle, Bad Actors employ cryptojacking malware on other people's computers. This malware forms a distributed attack network whereby unused processing power on victims' computers is harnessed to solve the crypto puzzle.

- *Data alteration/diddling*: If an attacker gains access to a database and changes a small amount of data every day for many weeks or months, it doesn't take long for the owner of the database to lose confidence in the entire database. Recovery by using a recent backup might not solve the problem, because it might require going back months to find untainted data; doing so, however, means the loss of all of the bona fide data entered since that clean backup was created.
- *Data breach*: Intentional or accidental release of information to an untrusted party.
- *Data leakage*: An inadvertent release of information learned by an attacker by inference; e.g., learning the parameters to a Web server script by looking at the page's source code or Uniform Resource Locator (URL), inferring the names of "hidden" files by examining the names of "visible" files, or learning secret information by combining multiple non-secret sources. Social media sites are excellent sources of data leakage and open source intelligence (OSINT).
- *Data theft*: Unauthorized access to data by a Bad Actor. Not the same as physical theft, where an item is taken away from the rightful owner with the intent to permanently deprive the rightful owner of possession of the item, because the data owner still has the data.
- *E-mail scams*: Frauds perpetrated by electronic mail, such as Nigerian 419 scams, bogus bills or invoices, fake warnings from credit card companies or the government, false customer support requests, etc.
- *Eavesdropping*: As the name implies, this is the passive interception of communication between two parties by a third-party.
- *Host exploit*: Use of malware or hacking tools that take advantage of one or more vulnerabilities in the operating system or applications software on a host computer or server.
- *Ineffective disposal*: Loss of sensitive information by ineffectively destroying unneeded data storage devices. As an example, many companies delete the files from end-of-life hard drives and then sell the hard drives on the Internet; unfortunately, data remains on a drive after being deleted and can be recovered by the next owner of the disk unless proper procedures are taken to truly clean the disk of all content. In fact, the most secure disposal method includes overwriting the drives with a random set of zeroes and ones, followed by physical destruction of the media.
- *Ineffective testing*: In the rush to get products to market and meet schedules, testing of hardware and software is often done superficially or incompletely. In some cases, with software, it becomes a matter of fixing flaws as they are found, after product release, by patching. In one famous case, a U.S. computer company outsourced its keyboards to a Chinese manufacturer. When the keyboards arrived, the computer company did functional tests to ensure that the keyboards worked as promised; only later did it learn that a keystroke logger was built into the keyboards, a piece of malware that transmits everything typed by users back to the manufacturer. In late-2021, a large U.S. payment processor discovered that point-of-sale (POS) terminals built by Chinese manufacturer PAX contained a repository of malware files and acted as a command-and-control center for staging attacks and collecting information.
- *Insider threat*: It is very difficult to build a system that protects against bona fide users with legitimate access to data. Disgruntled employees, spies, whistleblowers, or socially engineered users are all potential insider threats to the security of information.
- *Man-in-the-middle*: An active form of eavesdropping in which a third-party inserts themselves between two communicating parties, for the purpose of intercepting and, possibly, altering traffic between two parties of a communication session. In this case, the attacker masquerades as the other party to each of the victims.
- *Password spraying*: Whereas a *brute force attack* (see above) tries all possible passwords against one account, password spraying tries one password against all accounts before moving on to a second

possible password. The low-and-slow attack avoids some password-guessing detection methods.

- *Physical exploit*: Physical access to computers, servers, and other repositories of information is an important attack vector that is often overlooked in the pursuit of *cybersecurity*. There are many reported cases in which intruders walked into an office and walked out with a server containing tens of thousands of employee, customer, and financial records—generally unencrypted on the hard drive. Perimeter security, locked doors, restricted access, guards, cameras, and other physical barriers are imperative to strong information security.
- *Reconnaissance*: In order for a targeted attack to succeed, the attacker must learn as much as possible about the target organization. There are many ways to learn about the people (e.g., targets of social engineering or phishing) or networks (e.g., targets of hacking or DoS attacks) using public information, such as the organization’s own website, Internet search engines, online map sites, Wikipedia, social media sites, public business databases, Domain Name System (DNS) servers, and myriad tools that can find the network route of data or the geographic location of a company. Because this process uses public tools and servers, it is very difficult for potential targets to know when a nefarious reconnaissance is underway. Reconnaissance commonly relies on OSINT techniques.
- *Salami attack*: A form of financial theft in which the attacker steals extremely small amounts of money per transaction, resulting in cumulative sums of stolen funds that are very large. As an example: a programmer working in a bank is responsible for the program that calculates interest on user accounts. When the final digit in the amount of interest is greater than half-a-penny, the interest is rounded up and credited to the customer; when the amount is less than half-a-penny, the amount is rounded down and credited back to the bank. But an Evil Programmer could sweep the fraction of a penny to their own secret account. Over a period of time and a million or so of these transactions, the programmer might accumulate hundreds of thousands of dollars.
- *Session hijacking*: A form of attack where a third-party takes over a legitimate communication session between a user and a host. Session hijacking is widely used on the Internet when the user needs to be authenticated prior to accessing the host; the attacker takes over the session from the user after the user has been authenticated.
- *Supply chain integrity*: The supply chain refers to the set of companies, people, actions, information flows, and resources required to supply a product or service to a customer. From an information perspective, the integrity of the data flow among these disparate systems is critical. They must be synchronized to provide physical and digital assets at the right time and in the right place. From a cybersecurity perspective, we recognize that companies in a supply chain must necessarily have at least some access to a partner company’s network, thus becoming a potential threat, vulnerability, or attack vector, intentionally or otherwise. Maritime organizations are present everywhere in the supply chain, as an end-user/consumer, product or service supplier, and mid-point in other companies’ supply chains.
- *Unauthorized access*: Refers to any person or process that utilizes a resource without permission. Unauthorized access can refer to people entering a secured space within a building or facility, a user logging onto a computer account that is not their own, or an application using a network resource to which it should not have access.
- *Unpatched systems*: All computer operating systems (e.g., Android, iOS (formerly iPhone OS), iPadOS, Linux, MacOS, Unix, and Windows) and all applications are periodically updated with patches that add functionality and, ostensibly, improve security. For a number of reasons, uploading patches automatically across an entire organization’s network without management by the system/network administrator can cause more problems than it solves. On the other hand, unpatched systems remain vulnerable to new exploits. As one example: the Windows XP operating system reached end-of-life in April 2014. Many companies have not moved on to later versions of Windows, in most cases because they are using at least one application for which the vendor has not provided an upgrade path beyond XP. Those systems, of course, are unpatched and remain vulnerable to myriad exploits. While on this subject, note that Windows 7 support ended in January 2020.

A Worst-Case Scenario: Log4Shell

A fitting place to end this discussion seems to be with the Log4Shell vulnerability, found in a seemingly ubiquitous logging program and characterized as the single biggest and most critical vulnerability in a decade. Log4j is a Java-based, cross-platform logging framework developed by the Apache Software Foundation (ASF). Designed to provide a general mechanism for software to log actions and events on servers, it is used on tens of millions of

systems, including the very large base of Apache Web servers and more than 90% of Internet cloud services, such as Amazon Web Services (AWS), Cloudflare, iCloud, Minecraft, QQ, Red Hat, and Twitter.

In November 2021, a cybersecurity researcher discovered a vulnerability in Log4j that had been present for more than eight years. First privately disclosed to ASF, the vulnerability—dubbed Log4Shell—was publicly released in December. The vulnerability exploited Log4j allowing requests to be made to arbitrary Lightweight Directory Access Protocol (LDAP) servers without checking the response. This flaw allows an attacker to execute arbitrary code on the servers. It was given a score of 10.0 out of 10 in the Common Vulnerability Scoring System (CVSS) and described as a catastrophic design flaw. It was also almost immediately seized upon by cyberattackers, since more than 35,000 Java packages (Java classes and Application Programming Interfaces) are affected.

Log4Shell was a flaw in Log4j versions up to 2.14.1. After the disclosure of the vulnerability, Log4j version 2.15.0 was quickly released to address the problem. But then, an information leak and remote code execution flaw (CVSS score 9.0) was found that affected all versions up to 2.15.0; in response, v2.16.0 was released to fix that problem. Later, a denial-of-service vulnerability (CVSS score 7.5) was found and fixed in version 2.17.0. All of this occurred in just over a one-week period. New vulnerabilities have subsequently been found, an indication of just how difficult remediation will be, exacerbated by the constant round of updates that will need to be applied.

The story of Log4Shell will probably continue for some time. At a high level, it is an eight-year-old vulnerability that was suddenly discovered and turned into a series of zero-day exploits. But rather than a single fix, every new upgrade seemed to bring to light another vulnerability that increased the attack surface on Log4j and required yet another patch. Since Log4j is used on so many systems, it could take years before every vulnerable system is identified and upgraded, leaving a lot of systems—and time—for cyberattackers. Just prior to Christmas 2021, the national cybersecurity authorities in Australia, Canada, New Zealand, the U.K., and the U.S. released a joint cybersecurity advisory, a rare event that underscores the seriousness of this vulnerability.

Classifying the Cyberattackers

Not all cyberattacks—and, more importantly, not all cyberattackers—are created equal. Some companies suffer a cybersecurity incident because they are susceptible to whatever vulnerability is being exploited by the attacker; some companies are a specific target. In general, cyberattackers are categorized as follows:

- *Cyberactivists (Hacktivists)*: Like activists and protesters in the physical world, cyberactivists are generally motivated by philosophy, politics, and non-monetary goals. These hacking groups generally engage in activities such as social media disinformation campaigns and Web server defacements.
- *Cybercriminals*: Cybercriminals are motivated by the same thing as other criminals: money or other tangible goods. Cybercrime, including identity theft and ransomware, costs the global economy more than \$2 trillion annually according to some sources. Cybercriminal gangs might act for their own profit or hire out their services.
- *Cyberspies*: Acting on behalf of rival companies or nation-states, cyberspies engage in financial, industrial, political, and diplomatic espionage, including intellectual property theft.
- *Cyberterrorists*: These groups commit cyberattacks for political, religious, ideological, or social reasons, with the intent to promote fear in their target victims. Like terrorists in realspace, cyberterrorists might be independent individuals or groups, or working as proxies for a nation-state.
- *Cyberwarriors*: Also called information operations, these actors are part of a nation-state's military, and carrying out offensive and defense cyber actions to advance strategic goals. Cyberwar targets are generally military or critical infrastructures.

While a strict adherence to these definitions is not necessary when planning a cyberdefense, knowing something about the type of attacker gives a glimpse into their motivation, resources, and tenacity. It can also have some very practical implications, however. Lloyd's of London defines cyberwar as a cyberattack carried out as part of a war, in retaliation between nation-states, or that results in significant crippling in the functioning of a nation-state. In November 2021, Lloyd's released a set of exclusionary clauses whereby they would not cover cyberinsurance claims as a result of a cyberwar. Furthermore, even if such an attack could not be attributed to a source, Lloyd's reserves the right to apply a reasonable inference to determine whether an event is a cyberwar action or not.

Figure 2.2 shows the evolution of cyberattack tools since the introduction of the personal computer (PC) around 1980 to the present day. Many of these tools are freely available on the Internet and many others are available from hacker groups on the Dark Web. The main point of the chart is that the tools have, as expected, evolved tremendously from early command line tools to graphical user interfaces for Web-based and Internet-based hacking applications. These tools have become increasingly sophisticated and easy-to-use and, as a result, the knowledge required by someone to use them has decreased. By way of example, exploiting vulnerabilities in the 1980s required an attacker who was a programmer, largely writing their own tools, and with extensive knowledge of the target operating system. By 2010, the only skill required to use a vulnerability scanner was knowing how to use a Web browser.

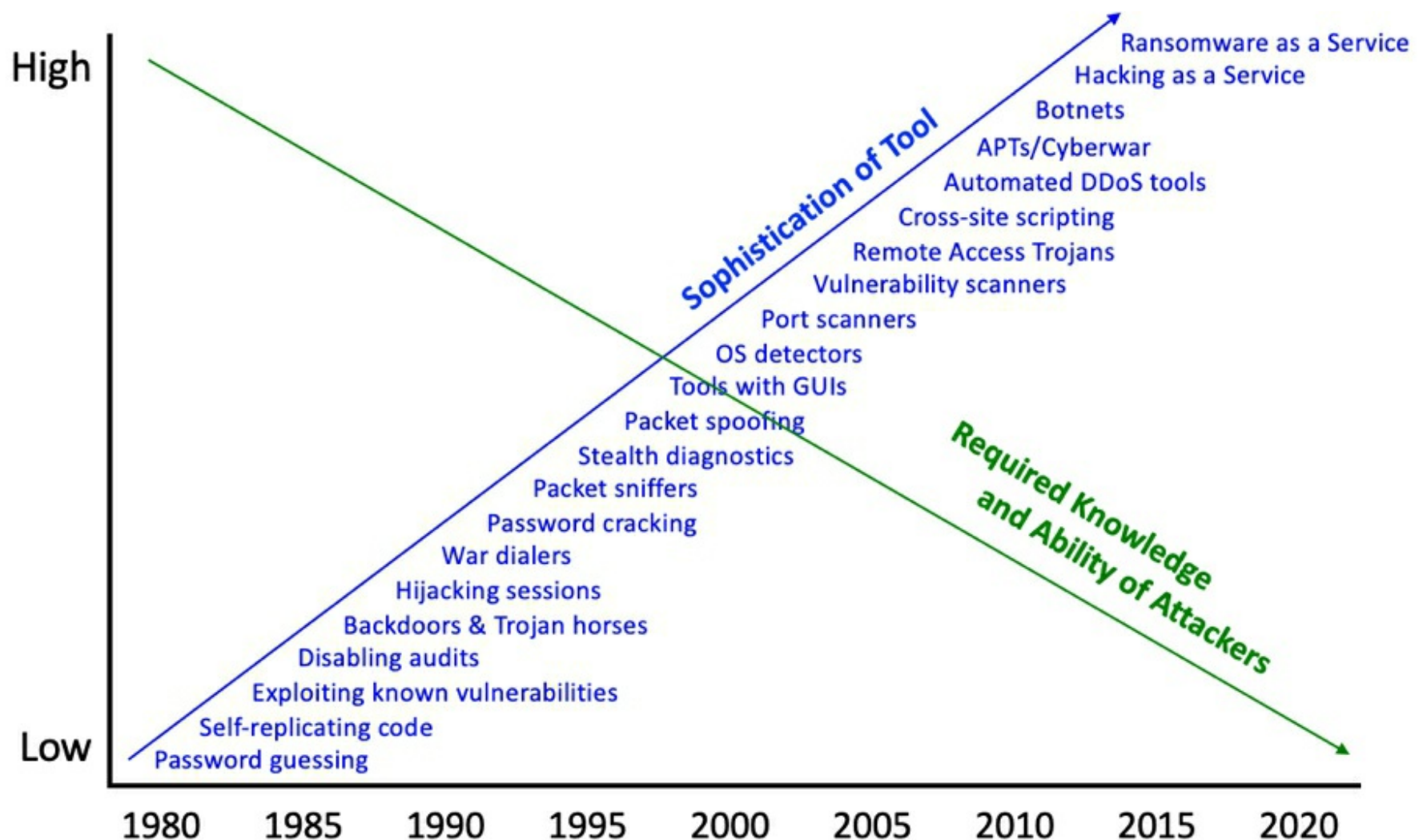


Figure 2.2. Evolution of hacking tools and techniques, and the required knowledge of tool users.

The significance of powerful tools that are easy to use is that they can be used to spread the “fog of war.” Consider again the Web-based vulnerability scanner. This tool is easy enough to use but still requires some advanced knowledge in order to fully understand, and exploit, the results of the scan. As a defender, you might see a hundred vulnerability scans targeting your site every day. One of those scans might have been conducted by an attacker performing a reconnaissance on your network in preparation for an attack, while the rest might be performed by pedestrian hackers who learned about the scanning tool in an online blog and have no idea what they’re doing. But as a defender, all you see are remnants of 100 potential attacks on your network.

Note also the entries for *hacking as a service* and *ransomware as a service*. Indeed, anyone can now hire a hacker to do their bidding, which requires no real skill at all.

Tools for Cyberdefense

This chapter has, so far, provided a long—albeit incomplete—list of cyberattack vectors. Rather than end the discussion here, it is important to note that there are some powerful tools available for information security managers to better detect and understand potential vulnerabilities in their systems, and plan their cyberdefense.

Software Vulnerability Databases

The Common Vulnerabilities and Exposures (CVE) Database^[3] is a repository of publicly known information security vulnerabilities. Currently funded by the U.S. Department of Homeland Security (DHS), the CVE database has been operated and maintained by The Mitre Corp. since 1999. The primary role of the CVE database is to provide a common terminology and reference methodology for researchers and cyberdefense tools.

A companion repository is the National Vulnerability Database (NVD),^[4] operated by the U.S. National Institute of Standards and Technology (NIST) Information Technology Laboratory. A CVE entry in the NVD contains details about the vulnerability, the software that is affected, the severity of the vulnerability, and suggested solutions and tools.

As an example, a search on the keyword *firefox* yields more than 2,750 CVE records. One of those entries, CVE-2021-38501, describes a flaw in Firefox's memory handling that could result in arbitrary code execution. The CVE database entry provides references about the vulnerability, and notes that this issue affects versions of the Firefox browser before 93 and versions of the Thunderbird e-mail client before 91.2. The CVE entry also points to the NVD entry, which goes into further detail about the severity of the vulnerability (this one has a score of 8.8 out of 10, which is a high risk flaw) and references to advisories and solutions.

Many automated software update and patching tools access the CVE database by use of a standard set of query/response programming primitives. Many organizations use a software inventory database; the automated patching tools uses the inventory entries as the search key into the CVE database and the mitigations in the NVD to keep the organization's software up-to-date and to minimize the vulnerability exposure.

ATT@CK[®] and D3FEND[™] Frameworks

The MITRE ATT@CK[®] Framework^[5] is a repository of tactics and techniques used by cyberattackers. This knowledge base is derived by observations in the real world, making this a valuable and practical tool for cyberdefenders and educators. An ATT@CK[®] matrix has been derived for enterprise, mobile, and industrial control system environments.

The ATT@CK[®] Enterprise Matrix, for example, lists 14 categories of tactics, including reconnaissance, initial access, execution, persistence, privilege escalation, defense evasion, lateral movement, command and control, and exfiltration. Within each tactical category are a set of attack techniques; in all, the matrix describes more than 220 attack technique categories.

Each technique is defined, along with a set of real-world examples, mitigation strategies, and detection methods. The Reconnaissance category, for example, lists 10 techniques, including active scanning, phishing for information, gathering the target's host, network, and organizational information, searching open websites, and searching the target's websites. Within each technique might also be sub-techniques, so that this category actually lists more than 30 attack methods. In all, the Enterprise Matrix describes nearly 600 individual cyberattack techniques.

Funded by the National Security Agency (NSA), MITRE's D3FEND[™] Framework^[6] is a knowledge graph of cyberattack countermeasures. The D3FEND[™] database maps cyberdefense methods to the various offensive tools and techniques identified in the ATT@CK[®] framework matrices. The D3FEND[™] database is organized into five areas:

- *Harden*: Approximately 20 methods with which to harden defenses in the broad categories of application, credential, message, and platform hardening.
- *Detect*: More than 55 defensive methods with which to detect an ongoing attack, in the broad categories of file, identifier, message, network traffic, process, and user behavior analysis, as well as platform motoring.
- *Isolate*: More than a dozen attack isolation methods related to process and network isolation.
- *Deceive*: Approximately 10 methods with which to deceive an attacker, including the preparation of a decoy environment and decoy objects.
- *Evict*: Three methods with which to expel an attacker by eliminating bogus credentials or malicious processes.

Each defensive method is defined, described, and, where relevant, mapped to related ATT@CK[®] techniques.

NIST Cybersecurity Framework

The NIST Cybersecurity Framework^[7] has emerged internationally as a common reference for many, if not most, cyberdefense guidance and best practices recommendations. The NIST framework is not a standard, but a voluntary framework of policy standards, guidelines, and best practices with which to assist organizations in assessing their ability to identify, detect, prevent, and respond to cyber incidents. The assessment also provides the organization with a plan to identify weaknesses in their cyberdefenses and a roadmap for improvement.

The NIST Framework is divided into three parts. The first part is the *core*, a top-down, hierarchical set of activities, outcomes, and references identifying approaches to building a cybersecurity plan. At the top level, the core is broken down into five functions (Table 2.2):

- *Identify*: Which processes and assets need protection?
- *Protect*: What safeguards are available?
- *Detect*: What techniques and practices can identify incidents?
- *Respond*: What techniques and practices can contain the impact of an incident?

- *Recover*: What techniques and practices can restore normal operations?

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 2.2. NIST Framework core functions and categories.

Each function is subdivided into categories that further identify the tasks to be performed to support the function. As an example, there are six categories that support the *Identify* function, including asset management, business environment, and governance. Each category has subcategories; the *business environment* category, for example, could address issues such as the organization's role in the supply chain, their role in the nation's critical infrastructure, or their ability to meet regulated resilience requirements. Finally, the subcategories can be mapped directly to other best practices, guidance, and standards documents from relevant organizations.

The second part of the framework is the *implementation tiers*, a way in which an organization can determine the context of how it views cybersecurity and, therefore, can design and plan an appropriate level of cybersecurity protections. This part of the framework provides a common terminology with which an organization can discuss the level of cybersecurity risk they are willing to accept, the priority of cybersecurity to the organization's management, and the available budget.

The final part of the framework are *profiles*, which are the mapping of an organization's understanding of their cyber requirements and objectives, risk acceptance level, and available resources (i.e., financial and personnel) to the desired outcomes described in the framework core. Profiles are useful in performing a gap analysis, helping an

organization to identify and prioritize ways in which to improve their cybersecurity posture.

NIST NICE Framework

The NIST Cybersecurity Framework describes technical aspects of building a cyberdefense strategy. NIST's National Initiative for Cybersecurity Education (NICE) Framework focuses on training and educating the cybersecurity workforce. By employing a combination of standards, common terminology, and best practices, the NICE Framework can be used by public or private sector employers defining the jobs of cyber professionals, academic institutions designing curricula that meet the needs of the industry, or students/trainees looking for a practical program of study.

The NICE Framework describes seven broad workforce categories, including *analyze*, *investigate*, *protect and defend*, and *securely provision*. Each category is composed of a number of specialty areas; as an example, the *protect and defend* category contains four specialty areas, including *cybersecurity defense analysis (CDA)* and *vulnerability assessment and management (VAM)*. In all, there are approximately three dozen specialty areas.

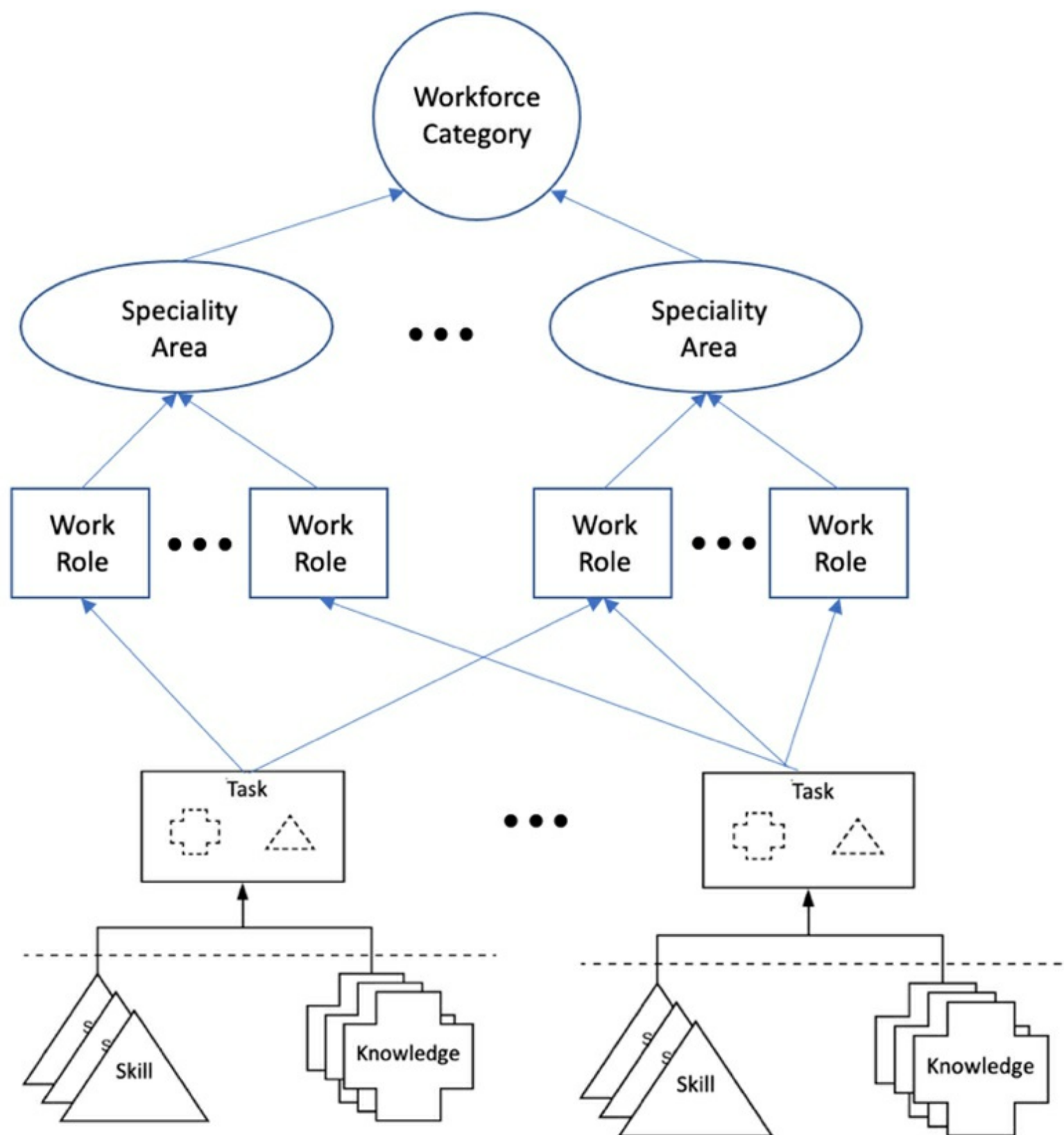


Figure 2.3. NICE Framework building blocks.

Each specialty area is associated with a work role, which is the descriptor of a job. Each role has a number of tasks that the job entails, and each task is defined in terms of the knowledge and skills that a learner preparing for this job—or a professional who holds this job—should possess. A task will comprise several knowledge and skill statements, and any given knowledge or skill might apply to multiple tasks and, by extension, to multiple roles (Figure 2.3).

The VAM specialty, for example, requires an individual that, among other things, can perform assessments of

systems and networks, and measure the effectiveness of cyberdefense strategies against known vulnerabilities. There are several tasks associated with this role, including the ability to analyze the organization's cyberdefense policies, conduct a penetration test, and maintain cyberdefense audit tools. The penetration test task, in turn, requires several knowledge areas (e.g., familiarity with application and network vulnerabilities) and skill areas (e.g., conducting vulnerability scans and recognizing vulnerabilities).

The NICE Framework is being adopted internationally and throughout the industry as a *de facto* standard describing jobs and academic programs. It provides guidance to both workers and learners about how to align the NIST Framework descriptions of cybersecurity policies and procedures to the practice of cybersecurity.

Zero Trust Architecture

In a traditional computing environment, trust might be extended to other devices for a number of reasons: the other device is a member of a “trusted” network, has previously been verified as a trusted device, or is employing an encrypted channel (e.g., a virtual local area network [VLAN]). *Zero trust*, on the other hand, means exactly what the words suggest, namely, the trust state of every device, user, and process needs to be reaffirmed every time one object attempts to access another object.

In a zero trust architecture (ZTA), both parties to a connection employ authentication to ensure that they have each verified the other’s identity, integrity, and access privileges, independent of location. Access to applications, processes, and network resources is based upon user authentication plus a high level of confidence in the other device’s identity, access rights, and integrity.

“Zero trust” has become a popular buzzword in the last few years but it is far from new. The concept—albeit not necessarily the practice—has been around for many decades and the term itself was introduced in the mid-1990s.

Applying Cybersecurity Requirements

The frameworks above are more than intellectual exercises; they are being incorporated into cybersecurity profiles, job descriptions, academic and training program offerings, and system implementations. Information security is also being made a part of contract requirements.

One example is the U.S. Defense Federal Acquisition Regulation Supplement (DFARS). As a result of a 2013 Presidential Executive Order named *Improving Critical Infrastructure Cybersecurity*, the Department of Defense (DoD) created the DFARS clause for the Federal Acquisition Regulation (FAR). This clause was designed to increase emphasis on cybersecurity compliance for DoD contractors and subcontractors, and utilizes the 110 controls defined in NIST SP 800-171, titled *Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations*. The 110 controls span 14 broad categories (called “families”), including access control, personnel security, physical protection, risk management, awareness and training, configuration management, identification and authentication, system and information integrity, and incident response. Note that the focus of DFARS is on information rather than on cybersystems, per se.

The DFARS Interim Rule specified that effective November 30, 2020, contractors and subcontractors must have a current gap assessment and system security plan uploaded to the Supplier Performance and Risk System prior to being awarded a DoD contract. Each of the 110 controls has been assigned a point value (either 1, 3, or 5 points) by DoD, and a NIST 800-171 assessment ultimately results in a score that ranges from -203 to +110. The methodology is that each organization starts at a perfect score of 110, and points are deducted for each control not met. The only exceptions to compliance with DFARS are commercial off the shelf products.

Looking forward, DoD is analyzing the use of the Cybersecurity Maturity Model Certification (CMMC). Like DFARS, CMMC is based on NIST 800-171. CMMC 2.0 is expected to be ready for implementation by 2024.

Conclusion and Summary

This chapter offers a broad overview of the cybersecurity threats that organizations face today. The threat and the challenges become broader and deeper every day. Bad Actors will take advantage of any attack vector that they can by sowing confusion, exploiting natural disasters, or moving quietly, while larger cyber campaigns are taking place. The COVID-19 pandemic is the most recent example of such disruption, where cyberattacks have dramatically increased to take advantage of corporate disorganization, heavy reliance on remote access to organizational resources, weaknesses in telecommuting and remote meeting software, inadequate funds to cover additional cybersecurity protections, and lack of central security management. Indeed, cyberattacks reportedly increased by 400% in the maritime sector alone between February and May 2020, the very earliest days of the pandemic.

As last food for thought for this chapter, we would like the reader to consider the following cybersecurity maxim:

Plug into the Formula Maxim: Engineers don’t understand security. They tend to work

in solution space, not problem space. They rely on conventional designs and focus on a good experience for the user and manufacturer, rather than a bad experience for the bad guy. They view nature or economics as the adversary, not people, and instinctively think about systems failing stochastically, rather than due to deliberate, intelligent, malicious intent. Being intelligent does not automatically make you think like a bad guy.

We rely on engineers and computer scientists to build systems that solve human problems or business needs. Cybersecurity experts always talk about thinking like the enemy (as Sun Tzu advises in *The Art of War*). The truth is that most engineers and programmers are woefully undertrained to think like an adversary. To do so, one must suspend a moral compass and focus on breaking things as fiercely as they thought about building them. In cybersecurity, in particular, nature is not the enemy; another person is.

In February 2017, the German government issued a rather strange mandate to the nation's citizens: If a child in your home owns one of the popular dolls called 'My Friend Cayla,' you are hereby ordered to destroy it. The doll, it turns out, listens to children, and then, using Bluetooth, connects to the Internet via a nearby iOS or Android device via the Cayla app, where it searches for keywords online so that it can parse them into full text responses to questions asked by a child.

As a demonstration of the Cayla doll's threat potential, Pen Test Partners showed how an attacker could easily use the Bluetooth connection, and the doll's on-board speaker and microphone, to communicate with children—as well as an unauthorized eavesdropping device. The doll's manufacturer shrugged off the hack as a prank, but the German government failed to see the humor, ordering the doll to be added to its list of unauthorized espionage devices under the German Telecommunications Act, given that it could be used to listen to any environment.

We mention this story because it serves as an exercise against the very real dangers of complacency. What possible damage could a harmless doll do? As it happens, a lot. A Bad Actor could easily exploit the doll to their advantage, all because its potential as an environmental penetration mechanism was dismissed due to its harmless appearance. Cayla is not a Trojan horse in the sense of a piece of computer code, but it is in the sense of a disguised penetration tool. *Caveat protector.*

Hopefully, the reader has concluded from this chapter that there is no such thing as a completely impenetrable system. As networks and the computers connected to them become increasingly capable, they also become increasingly complex. With that capability and complexity comes a vastly expanded attack surface which Bad Actors are all too happy to exploit. And while completely safe computer systems and networks don't realistically exist for all the reasons cited in this chapter, they can be made more secure.

Think about a robber casing a neighborhood for potential targets. One house is brightly lit, has a perimeter and intrusion alarm system, and all the doors and windows are locked. A large, noisy dog roams the backyard. Another house is dark, bushes are overgrown to the point that the backyard cannot be seen from the street, and two windows are ajar so that fans can be placed in them. And, there is no sign of a pet. Both houses are equally attractive in terms of what could be stolen, but which one is the robber most likely to enter? The point, of course, is that Bad Actors will typically go after the softer targets. The more difficult a system is to penetrate, the less likely it is to be targeted.

There is a joke amongst SCUBA divers about the real reason we dive with a buddy. If a man-eating shark approaches the buddy pair, one diver only has to outswim the other; they don't have to outswim the shark.

The next chapter examines some case studies of actual cyberattacks in the maritime sector. We'll cover additional case studies for the next several chapters and then start to present some mitigation strategies. Do not fall into the trap, however, of believing that future cyberattacks are somehow constrained by the past. If one can imagine a method for a cyberattack, that method is probably feasible—if not today, then sometime in the future. Think like an attacker, not a defender.

Chapter 3: Case Studies—Cyberattacks on the Maritime Sector

Introduction

In the previous chapter, we offered a broad overview of the different types of potential cybersecurity attacks. In this chapter, we present case studies of actual cyberattacks in the maritime sector to bring the theoretical and “merely possible” into the realm of practical and real. The case studies described here are not exhaustive and contain only information that is in the public domain. They will, however, provide the reader with a sense of the breadth and depth of the challenges presented by current cybersecurity threats. The case studies presented here do not include attacks focused specifically on ports, as port cybersecurity is the subject of the next chapter.

Malware Attacks

Once installed on an organization’s computers, malware presents an enormous cyberthreat that is not protected by any of the network’s perimeter security. Malware can be introduced into an organization in a number of ways.

One early malware attack in the maritime sector affected a new build offshore drilling rig after it left its construction site in South Korea in 2010. Neither the maritime sector nor drilling platforms were targeted in this attack, yet the platform nevertheless became overwhelmed by malware while en route to its drilling location. The most likely scenario is that one of the many computers on board was victimized as part of a larger malware campaign, and the malware then spread to other systems on the rig. Among the infected computers on the drilling rig was the blowout preventer (BOP) system which, if infected, could have led to an explosion, had the rig actually been drilling. Once on-site, the platform was shut down for 19 days so that the malware could be purged from the systems and network.

Stuxnet, a Microsoft Windows-based worm, was discovered in 2010, and is possibly the first publicly-known malware intended to damage hardware. The Stuxnet worm employed several zero-day exploits and specifically targeted Siemens Step7 software, the Windows application that controlled a particular model of centrifuge known to be used at Iranian uranium enrichment facilities. The worm was believed to have been introduced via USB thumb drives, but also propagated via local networks and, presumably, the Internet. Stuxnet was a computer worm, a form of malware that is close to impossible to control once it is released into the IT wild. While Stuxnet targeted Siemens centrifuges in Iran and destroyed as many as 25% of the Iranian nuclear-related centrifuges, only 60% of the systems affected by Stuxnet were actually in Iran; another 18% were in Indonesia and 8% in India.

In 2012, Chevron revealed that the Stuxnet virus had been found in its industrial control networks, albeit with no damage discovered. It is not known whether there was any impact on Chevron’s maritime facilities, but it is clear that an attack like this can have serious unintended consequences.

One of the most common mechanisms by which malware is distributed is software posted on questionable websites. Another oil rig, this one in the Gulf of Mexico, was infected with viruses that came from infected pornography and music files downloaded by workers. Once it was on one of the rig’s systems, the malware moved from computer to computer. Although the crews work grueling 14-hour days, they still have downtime when they use their computers—and there are more than 2,000 offshore platforms in the Gulf alone. While this example is specific to oil platforms, it is by no means limited to them; consider the similar environment that exists with the crew of a merchant vessel.

Rate request sea freight import from Warsaw, Poland upto Shenzen, China

To: undisclosed-recipients;

Good day,

Please advise as per below rate request.

We have an urgent Sea Freight import freight request on FOB Basis as per following shipment details.

POL : Warsaw, Poland
 POD : Shenzen
 Equipment : 1X20'FCL & 1X40 HQ
 Commodity : General Cargo
 Weight : Normal
 Terms : FOB
 Readiness : 1st week of june 2019.

Please see attached additional shipment details for your perusal. We require the following information.

- a) Ocean Freight on Multiple shipping lines, along with routing & Transit time and rates validity.
- b) Kindly confirm 14 free days at POD

We will really appreciate your prompt action in this regard

Thanks and Best Regards,

Esther Yan / Marketing

?????????(??)?????????
 GLOBAL GOODWILL LOGISTICS CORP (SHENZHEN OFFICE)
 ?????:????????????????????1906?(?????????)
 ROOM1906, INTERNATIONAL CHAMBER OF COMMERCE TOWER, FUHUA RD.3, FUTIAN, SHENZHEN, CHINA
 TEL: 86-755-88312836 EX: 125
 FAX: 86-755-88312677
 E-mail: esther.hui.yan@formosa-sz.cn
 Skype: hui-yan



Website: www.formosatwn.com.tw IMPORT_SEA
 FREIG..._zip.arj

Figure 3.1. Suspicious e-mail with suspicious attachment.

A second major method by which malware is introduced into a computer system is when users open e-mail attachments. Figure 3.1 shows a suspicious e-mail received by one of the authors. At first glance, the e-mail seems to be a request for a quote to ship material from Warsaw, Poland to Shenzhen, China. This is actually a pretty good quality spam/phishing message. The item that should give the user pause is the attached file. Even if a file attachment is the standard method used to send the information necessary for a quote—and it definitely should not be—the filename (*IMPORT_SEA_FREIGHT_FOB_zip.arj*) should create suspicion.

Maersk Line <finance@tsakerr.com> 

Inbox - GCK April 07, 2021 at 13:13 PM

ML 

Export Invoice // BL draft copy // shipping documents

To: Dr. Gary C. Kessler <gck@garykessler.net>



Dear Consignee,

This is to notify you of a shipment assigned to you as the recipient.

Please see attached BL Draft Copy and Shipping Documents at the request of our Customer and confirm details for approval.

Awaiting your response.

Best Regards

Mary Cheng



Maersk_BL
Draft_c...ts.html

Figure 3.2. Suspicious e-mail with link to a website.

As anti-malware software gets better at finding suspicious content in file attachments and bogus URLs, and users become more wary about opening these files or clicking, the cyberattack tactics change. Figure 3.2 shows another e-mail received by one of the authors. In this case, the e-mail appears to come from Maersk with a message about some shipping documents. Note that while the e-mail purports to come from *Maersk Line*, the actual address does not appear to be from a Maersk domain. In this case, the attachment is an innocuous Hypertext Markup Language (HTML) file (Figure 3.3) that appears to be an e-mail login page from where a user can obtain the promised files. This is a classic *credential harvesting* attack; after the user enters their e-mail address and password, the attacker captures that information for their own use later. To allay suspicions, the user is allowed access to files that may or may not contain malware.

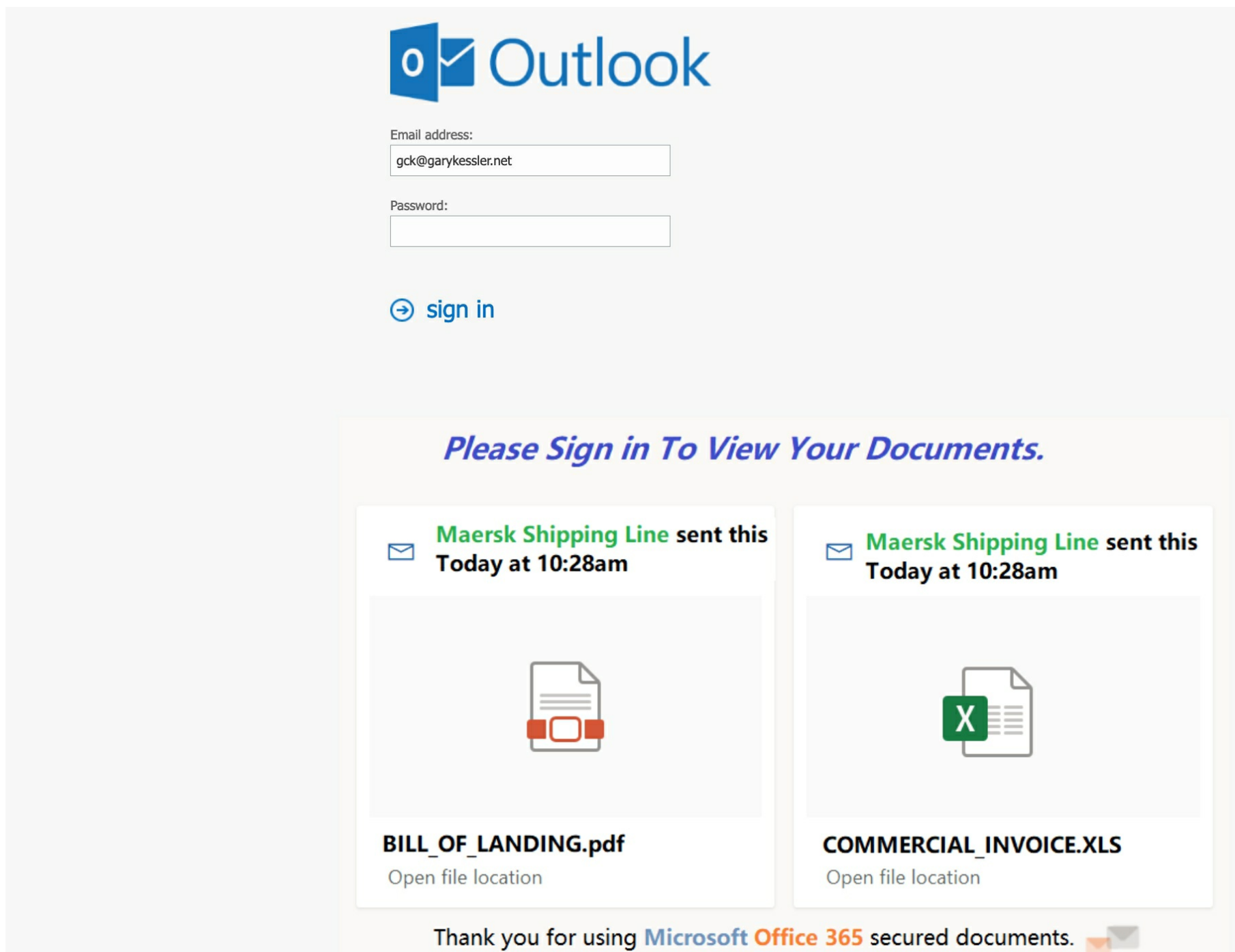


Figure 3.3. Website link from suspicious e-mail.

Many malware distribution schemes, such as the one just described, target maritime assets. One spearphishing campaign took aim at ports using a malicious attachment that contained the Emotet Trojan. This executable attachment, once clicked, acts as a loader on Windows systems, updating Registry settings and starting several Windows services. The malware can then spread to other computers on the internal network via open network shares and outside of the local network by sending spam to addresses in the infected computer's address book. The malware can also communicate back to a command and control server run by the Bad Actor who started this thread of spam, effectively making the targeted computer part of a nefarious botnet. Finally, it can also download other malware, such as the Dridex Trojan. Dridex rose to become one of the most prevalent financial and banking Trojans by 2019, attacking both the financial services sector and banking customers. Dridex and its variants, once installed, affect the confidentiality and availability of customer data, as well as the availability of computer systems themselves.

A similar malware spam campaign targets maritime (and other) shipping companies. These e-mails, with subject lines similar to "Shipping docs#330," contain bogus shipping documents in file attachments with names such as *DOC000YUT600.pdf.z*. A "Z" file extension indicates a compressed file. When decompressed, the attachment contains a file such as *DOC000YUT600.scr*. The SCR file is a script which, when executed, installs the DarkComet Remote Access Trojan (RAT). This program runs automatically when the user logs into Windows; the RAT can log keystrokes, monitor application usage, take screenshots, delete files, allow remote logins, and steal a significant amount of information from the infected system.

In June 2021, Hyundai Merchant Marine (HMM) e-mail systems were compromised by a "virus attack." It was reported that the attack exploited an unpatched Microsoft Exchange Server zero-day vulnerability that became known two months earlier. Combined, there were four vulnerabilities that allowed attackers to authenticate as the Exchange server, run code at System level, and write files anywhere on the server. The campaign was attributed to Hafnium, a Chinese state-sponsored APT group.

Cyberattacks and Hacking

One of the first publicized cyberattacks on a shipping company occurred in 2011 and targeted the Islamic Republic

of Iran Shipping Lines (IRISL), owner of the largest fleet in the Middle East at the time. During a period of international sanctions and a high level of diplomatic tension, IRISL's network was hacked, taking down logistics systems and compromising the entire fleet of more than 170 vessels. The attackers fed false information into systems, creating bogus manifests, rate information, delivery dates, and delivery locations. Client and vendor information was also altered, and all ship tracking was lost for some days. In addition to huge financial losses for IRISL, some cargo was never found—it just disappeared. The source of the attack was never definitively attributed, although politics is thought to have been the motivation.

Pirates have also become more high-tech in their efforts to optimize operations. Hackers working with pirates have myriad sources of information (often shipping company or vessel insiders), motives (financial, political, or ideological), and targets (more than 60,000 merchant vessels carrying the world's cargo). Pirates might direct their cyberattacks at the vessel itself, the cargo, or just to demonstrate that it can be done. In one early incident in 2016, pirates hacked into a shipping company by exploiting a vulnerability in their content management system. Rather than crash the system or take any actions that attracted attention, they created a backdoor^[8] that allowed them to access shipping route, schedule, and container content information whenever they wanted over a period of many months. The pirates then targeted specific ships and, using barcode readers, targeted specific containers once aboard the vessel. In these attacks, the pirates were on and off the ship in a matter of hours and were able to get exactly the cargo they sought.

The maritime industry has suffered many data breaches in which attackers target corporate or employee information. In March 2018, Svitzer, with 4,000 employees in 34 countries, learned that attackers had entered their e-mail server 10 months earlier (May 2017). The attackers identified three employees in Australia who worked in finance, payroll, and operations. By setting a standard Office 365 auto-forwarding rule, all 50,000-60,000 e-mails received by those employees during that 10-month period were forwarded to two external accounts without the knowledge of the account holders. Svitzer, a part of the Maersk Group, lost sensitive personnel information for about half of their 1,000 Australian employees.

In April 2020, the Mediterranean Shipping Company's (MSC) website was subjected to a malware attack reportedly limited to a single server in Geneva, Switzerland. As a result, MSC's website and booking systems were down for most of a week. The attack, and the fact that the *MyMSC* portal was down, demonstrates the potential impact of an attack on a shipping line's passenger or cargo reservation system, which contains individual identification and credit card information, employee data, route scheduling, food and fuel costs, crew placement, and more.

In September 2020, Red Funnel, a U.K. ferry operator connecting Southampton with the Isle of Wight, was the target of a cyberattack. In this case, critical IT systems were brought down for several days, affecting online booking and scheduling, and customer account inquiry systems. The attack appeared to be malicious in nature with a goal of straining the network and taking systems down rather than data theft.

In March 2021, the e-mail system at the China Ocean Shipping Company (COSCO) was brought down for several days as the result of a cyberattack. The attacker—reportedly a Brazilian hacker called L0RDBR—exploited a known flaw in Microsoft's Exchange and Outlook software, for which a patch had been released a week earlier.

In unrelated cyberattacks, both Carnival Cruise Lines and Kawasaki Kisen Kaisha (K Line) also suffered data breaches in 2021.

Cyberattacks, of course, are not limited to shipping lines. Australian ferry and defense shipbuilder Austal was hit by a cyberattack in late 2018. The unknown attacker was able to penetrate its data management system and steal internal data, including contact information and unspecified data affecting customers and fabrication sub-contractors, and ship design drawings that were said to be neither classified nor sensitive. The attacker also attempted extortion of the company by threatening to sell some of the stolen data online, but Austal refused to pay any ransom.

In October 2020, the International Maritime Organization (IMO) was the target of a sophisticated attack that successfully bypassed dynamic cyberdefenses. IMO's public website, intranet, and other processes were offline for several days, most likely due to an outdated version of the Microsoft SharePoint Web server.

Smartphone maritime apps are also subject to cyberattack. In October 2018, Navionics, a subsidiary of Garmin, was found to have a misconfigured database server connected to the Internet. A cybersecurity researcher came across Navionics' MongoDB server and found that it was not configured to use password protection, making its entire 19 gigabyte (GB) database openly available on the Internet. The researcher immediately notified Navionics and the problem was fixed, but it took several weeks for the problem to be reported, investigated, and resolved. The database contained more than 261,000 customer records including names, e-mail addresses, product and user IDs, and boat information (e.g., latitude, longitude, course, speed), although it was reported that no data was exfiltrated.

Cyberfraud and Phishing

Many maritime companies are susceptible to phishing scams and other frauds because of the high volume of communication, orders, and financial transactions that occur online. Some of these frauds occur through the use of bogus e-mail scams, some by phishing, and some by manipulating industry-standard electronic invoicing documents, such as *International Forwarding and Transport message - Freight Costs and other Charges (IFTFCC)* and other messages.

One such fraud was perpetrated against fuel bunker company World Fuel Services (WFS), headquartered in Miami, Florida. In October 2013, criminals using a bogus supply tender from the U.S. Defense Logistics Agency (DLA) ordered 17,000 metric tonnes of marine gasoil (MGO) from WFS. WFS, in turn, contracted with a fuel supplier, Monjasa, to deliver MGO to vessel OCEAN PEARL off the coast of Togo in the Gulf of Guinea; this transfer of fuel occurred in early December. Later that month, WFS sent an invoice to DLA for \$17.9 million and, in January 2014, paid Monjasa \$17.1 million for the fuel. Later in January, WFS followed up with DLA for payment, and was later advised by the FBI that they had been defrauded. While insurance covered most of WFS' monetary loss, the MGO was never located or recovered.

Malware was a part of another bunker company fraud in 2017. Spyware was embedded into a computer system at a bunker company in Malaysia, allowing Bad Actors to read the e-mail exchanges between the company and its fuel suppliers. After obtaining sufficient information, the cybercriminals were able to set up a bank account that allowed them to spoof one of the bunker company's real fuel suppliers in Singapore. The Malaysian bunker company was deceived into transferring \$1 million to a bank in Greensboro, North Carolina to pay the Singapore fuel company for actual fuel deliveries. The bunker company did not know of the fraud until the fuel company followed up for payment of its invoice.

An equally elaborate multi-party fraud occurred between a shipbuilder and a marine escrow company in November 2014. Dubai-based Marine Assets Corporation (MAC) entered into an agreement with Fujian Mawei Shipbuilding, a Chinese shipbuilder, for the construction of a vessel to be deployed in 2018. Canadian mineral exploration company Nautilus Minerals paid \$10 million to MAC as a deposit on an \$18 million charterer's guarantee for the newbuild vessel. In December, Nautilus discovered that an unknown party had hacked into both Nautilus' and MAC's computer systems, causing Nautilus to transfer the \$10 million into an account that it erroneously thought belonged to MAC. The vessel construction and charter plan continued to move forward, but the \$10 million was never recovered.

Figure 3.4 shows an e-mail received by one of the authors in 2018 that contains several of the red flags that indicate an attempt to distribute malware, as discussed earlier in this chapter. While this message is rife with warnings that we have seen before, the most glaring and suspicious indication of fraud is the reference to the use of an alternative e-mail address.

Using this very tactic, a shipping company in Limassol, Cyprus was defrauded by cybercriminals masquerading as a legitimate bunker company. In July 2015, the shipper received an e-mail from their African fuel supplier with an invoice for €565,000 (\$644,000) and, most notably, with a *request for payment to go into a different bank account than its usual one*. The shipping company made two bank transfers to the criminal's bank account, and the money was never found or recovered.



payment advice

To: undisclosed-recipients;;

Dear sir,

We are writing from our alternative email as our email server is under maintenance, please kindly forgive us for delay in payment.

Find the attached payment slip as we made the transfer on 14th june, 2018.
your earliest confirmation will be very much appreciated.
If you have any question don't fail to contact us.

Thanks & Best Regards,
Kase

Accounts department
Diana Kase(Ms)

ny73103@imexgroup.am



+++++ PAYMENT_ADVI
CE-PDF.ARJ

Figure 3.4. Bogus e-mail with attachment, coming from sender's "alternative email."

Deceptive e-mails are also the heart of phishing campaigns. The social engineering aspect found in the content of these e-mails is often hidden by the fact that people increasingly read their e-mail on the small screens associated with cell phones, tablets, and other mobile devices. In March 2020, Holland America Line and Princess Cruises (both Carnival Corp. passenger lines) reported that they had been victimized by a phishing attack in May of the previous year. Phishing e-mails sent to employees ultimately allowed an attacker to access employee e-mail accounts. In turn, the Bad Actors were able to access employee and customer personal information, including names, Social Security and other government identification numbers, passport numbers, credit card and financial information, and PHI.

In an example of phishing being employed by a nation-state for cyberespionage, a Chinese APT group attacked a Russian Navy submarine designer in 2021. A spearphishing e-mail campaign specifically targeted a general director at a Saint Petersburg defense contractor responsible for designing most of Russia's nuclear submarine fleet. A weaponized Rich Text Format (RTF) document that ostensibly contained the plans for an autonomous underwater vehicle was sent as an attachment to the company's CEO. When opened, the document dropped the PortDoor malware in the Microsoft Word startup directory. PortDoor is malicious backdoor software that can be used by an attacker for reconnaissance, system profiling, command and control payload distribution, privilege escalation, evasion, encryption, and data exfiltration.

Ransomware

One of the most notorious cyber events in the maritime industry is the ransomware attack that impacted Danish shipping company A.P. Møller - Maersk in 2017. Most noteworthy, given the damage done, is that Maersk was not a target of the attack; it was merely susceptible. Maersk runs a huge operation: it is responsible for 76 ports around the world and operates 800 vessels carrying tens of millions of tons of cargo every year. A ship in Maersk's fleet enters a port every 15 minutes somewhere in the world; its vessels represent nearly 20% of the world's cargo shipping capacity.

The genesis of this story has nothing to do with Maersk or the maritime industry. In April 2017, a hacking group called The Shadow Brokers provided a large number of cyber exploit tools—allegedly created by the CIA and NSA—to WikiLeaks. One of those tools was called EternalBlue, an exploit for a vulnerability in the Server Message Block (SMB) service in the Microsoft Windows operating system.^[9] Although Microsoft had already released a

patch for this vulnerability in March, the patch had not been universally applied by the user community. In addition, Microsoft did not release a patch for discontinued versions of Windows, including Windows XP; while still widely used in 2017, XP's end-of-life was in April 2014.

The first EternalBlue-based cyberattack occurred in May 2017, when the WannaCry ransomware worm began to circulate on the Internet. This was the scenario presented in Chapter 2 of this book. In the first 24 hours, tens of thousands of computers in 99 countries throughout the Americas, Asia, and Europe were infected with WannaCry; by the end of the second day, more than 230,000 computers in 150 countries were infected. WannaCry did not specifically target any of its victim sites; it was a worm that traveled around the Internet, infecting vulnerable systems, including nearly 80% of the U.K.'s National Health System (NHS) computers that were using Windows XP. WannaCry died down within a few days after two defensive actions were taken: Microsoft released an emergency patch for older operating systems, and a cybersecurity researcher found a "kill switch"^[10] to stop WannaCry from propagating. Most of the victim sites were running the Windows 7 operating system.

Threats from EternalBlue were not over, however. In June, cyberattackers released a new worm using the EternalBlue exploit, called NotPetya. At this point, there remained hundreds of thousands of unpatched Windows systems around the world. While WannaCry appeared to be ransomware launched by cybercriminals, NotPetya appears to have primarily targeted sites in Ukraine, designed to destroy files and computer systems.

One victim of NotPetya was Maersk, whose IT systems were shut down network-wide, including their terminal in the Port of Los Angeles. All of Maersk's Active Directory (AD) network domain controllers were compromised except for one in Ghana that happened to be off-line at the time of the attack due to a local power failure. Employing that one server, Maersk was able to rebuild its entire AD domain controller network. The company replaced its entire network of more than 45,000 computers and 4,000 servers; its systems were down for 10 days, and the company experienced a revenue loss estimated at more than \$300 million.

While this is one of the best-known and most often-cited ransomware attacks in the industry, it is important to note that Maersk was not a deliberate target of NotPetya, but merely susceptible to the EternalBlue exploit. Nevertheless, it was a harbinger of things to come. In the summer of 2018, the U.S. division of COSCO was struck by a Windows-based cyberattack, affecting the company's internal network and e-mail system. Rather than contact customer service agents via phone or e-mail, customers were advised to use the e-commerce function of the COSCO website for booking requests, shipping instructions, etc. On the first day of the attack, COSCO was forced to shut down its terminal at the Port of Long Beach; by the second day, widespread network failure across COSCO Americas disrupted e-mail, local websites, and telephone systems in Argentina, Brazil, Canada, Chile, Panama, Peru, U.S., and Uruguay, and the shipper was forced to temporarily suspend hazardous and awkward^[11] cargo bookings. Some employees started to use non-COSCO e-mail accounts to contact customers, which is, ironically, a red flag for potential cyberfraud (as noted above). While the complete details of the attack have not been publicly released, this was, at least in part, a ransomware incident. COSCO's global fleet of more than 1,100 vessels was reportedly not affected.

Ransomware attacks have continued to increase in number and the year 2020 saw maritime and maritime-related companies increasingly being targeted:

- In January 2020, Toll Group, an Australian transportation and logistics company, was hit with the Mailto ransomware; in May, they were hit by the Nemty ransomware. In both cases, the MyToll customer portal was taken offline and the May attack was exacerbated by work slow-downs caused by COVID-19. Toll has 1,200 locations in 50 countries.
- In June, Vard Group, a Norwegian shipbuilder, was struck by the Sodinokibi ransomware. Already hurt by the COVID-19 pandemic, the attack resulted in layoffs at its shipyard in Langsten.
- In July, Garmin was hit with a ransomware attack that left its fitness tracking apps, customer service infrastructure, and most real-time services offline for several days; its aviation services were possibly the hardest hit. Although ship- and military-related services were reportedly unaffected, many of the affected services are used by members of the maritime industry. Garmin reportedly paid a \$10 million ransom to get back online.
- In August, Carnival Corp. suffered a ransomware attack that resulted in the loss of an unknown amount of employee and passenger personal data. Carnival employs more than 150,000 personnel and, prior to COVID-19, had approximately 13 million passengers per year on its 10 cruise lines.
- In September, French container carrier CMA CGM was struck by the Ragnar Locker ransomware. As a result, the websites of CMA CGM and two subsidiaries, Australian National Lines (ANL) and CNC, were taken offline, and order-taking and cargo handling were greatly slowed.
- In December 2020, Norwegian cruise line Hurtigruten was hit by ransomware. The attack affected its entire worldwide network, compromising customer PII.

- Later that month, AIDA Cruises was struck by the Doppelpaymer ransomware. The attack resulted in the failure of the company's land-based and shipboard telephone, computer, and Internet systems, and forced the cancellation of several voyages.
- In June 2021, the network of the Woods Hole, Martha's Vineyard, and Nantucket Steamship Authority (SSA) in Massachusetts was brought down by ransomware. The SSA provides all transport of people and goods to the island of Martha's Vineyard. The regular reservation and ticketing systems were disrupted for 10 days.
- In October 2021, ransomware spread through multiple Greek shipping companies through systems operated by Danaos Management Consultants, a well-established IT consulting firm offering services to the maritime industry since 1986. Danaos Maritime Software Suite ship management software functions include chartering, payroll, crewing, analytics, document management, procurement, and online collaboration.

Information Leakage and Open Source Intelligence

Information leakage is not a cyberattack, per se, but refers to ways in which the industry inadvertently releases information that a Bad Actor can use to attack maritime assets. Open source intelligence, which can include information leakage, refers to the use of public information databases to learn about a company, person, or organization.

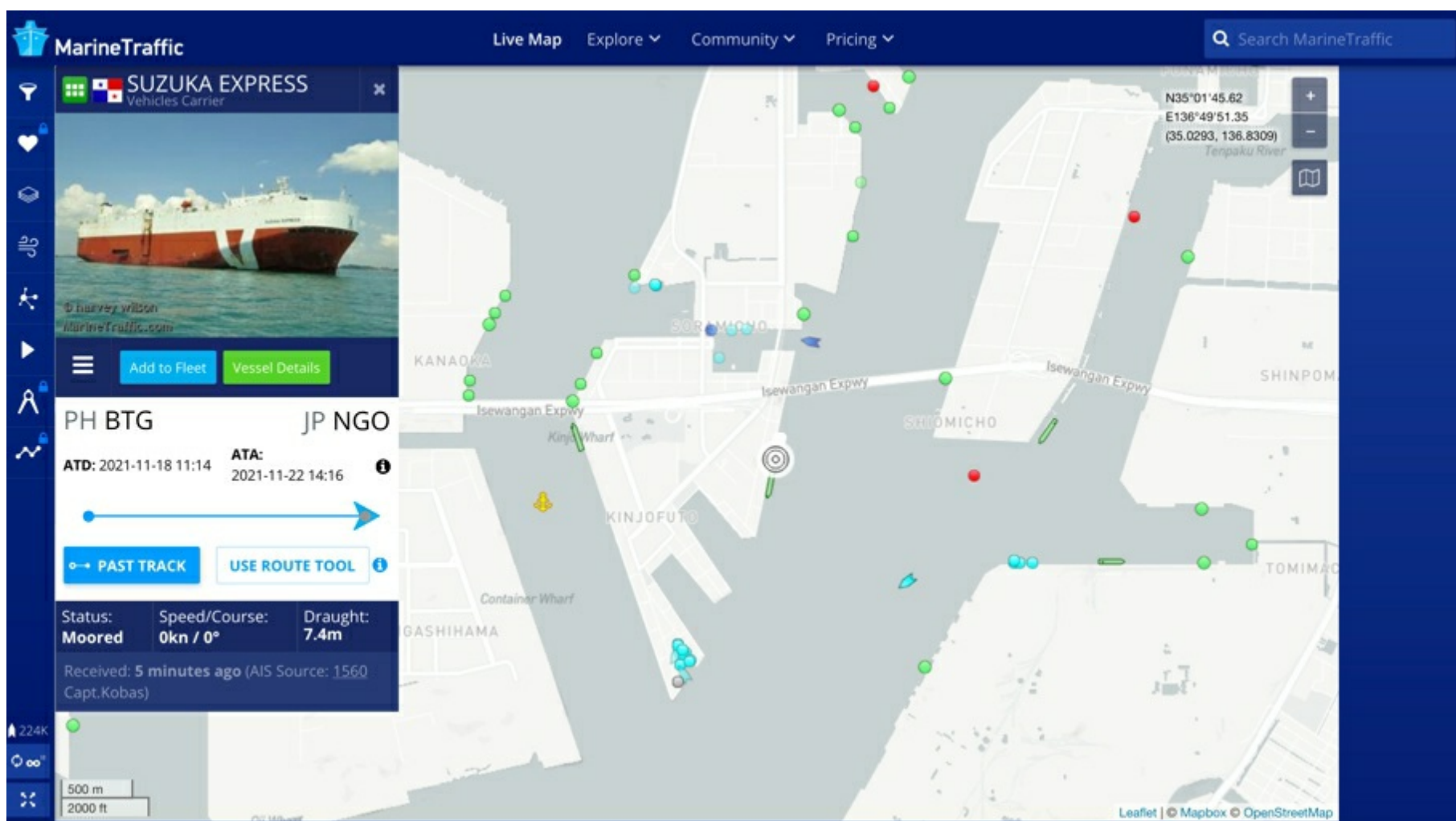


Figure 3.5. Location of SUZUKA EXPRESS on 22 November 2021.

One such example of public databases, as described at the beginning of this book, are the many sites that track the location of commercial, recreational, and other vessels around the world. This information is gathered from ships that broadcast their Automatic Identification System location information, per international safety regulations. There are a number of vessel tracking sites on the Internet, including CruiseMapper, MarineTraffic, Shiptracker, and Vesseltracker.^[12] A large amount of vessel information is readily available to anyone with access to the Internet. As an example, Figure 3.5 shows the location and other information for vehicle carrier SUZUKA EXPRESS per MarineTraffic, a website with nearly one-and-a-half million records in its vessel database.

Email or Profile no. Password

Remember me [Forgot Password / Profile No.?](#)


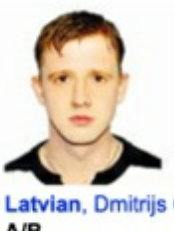










Nationalities ▶ All 286565 seafarers ▼


Mates 286 565
Seafarers, cadets of all nationalities and ranks


Ships 115 278
Cargo, offshore, cruise, platforms, inland ships


Crewing Agencies 2 348
Your profile is your application

Invitations to work 4 765
[Registration for agencies, crew management companies, shipowners here»](#)

 SYDSTRAUM	 Latvian, Dmitrijs O. A/B	 SEA FLYER	 Ukrainian, Artem Electric Officer	 MSC MELODY	 Romanian, Anca Photo Staff
 MAERSK SERVER	 British, Simon Peter Chief Officer	 SANDERUS	 Dutch, de Ruiter Master Mariner	 MAERSK STEPICA	 Dutch, Wilson 3/Officer

CMB CORALIE 
Filipino, Chris Johr
Chief Officer

GASCHEM WERRA 
Polish, Artur
Chief Engineer

COLUMBA 
German, Svenja
2/Officer

19:07 GMT
Monday, 22 November

©MyShip.com mission is to discover new generation of professional seafarers. MyShip.com like Neptune's trident has three dentes (teeth) that represent seafarers of all nationalities, crew companies from around the world and all ships in one social networking website. [Join us today](#) | [Contact for seafarers](#) | [Contact for agencies](#) | [Forum](#) | [Sitemap](#)



Figure 3.6. MyShip social and career website for merchant mariners.

Now, couple this with social and professional networking sites directed at the merchant mariner community, such as *Maritime-connector.com* and *MyShip.com* (Figure 3.6). By insinuating themselves onto these sites, cybercriminals, cyberstalkers, or other Bad Actors can socially engineer information from unsuspecting mariners, motivating them to innocently give up information about routes, cargo, arrival times, port security procedures, standard operating procedures of ships and ports, and more.

Sometimes, information is leaked voluntarily, albeit inadvertently. In order to deny pirates access to actionable intelligence, for example, many ships will disable AIS or send bogus AIS data, or post misinformation on official social media outlets. These efforts might be undermined by crew members who upload information to their personal social media pages, sometimes compromising the safety of the vessel. It's no secret that people are often the weakest link in the cybersecurity chain of responsibility: Mariners—from the ship's master to an apprentice seaman—are *de facto* guardians of billions of dollars' worth of cargo and equipment, and are therefore responsible for maintaining the integrity of the MTS.

Many vessels have their own officially sanctioned websites and social media presence. These sites, too, provide the opportunity for information leakage—and targets for cyber-attack. In October 2021, for example, the Facebook page for the USS KIDD was compromised when a hacker took over the page and streamed the real-time, online, multiplayer game, *Age of Empires*. In this case, the U.S. Navy lost control of the page as unauthorized users posted unauthorized content about the vessel.

There is a large amount of OSINT that can assist an attacker to perform a basic reconnaissance on a potential maritime target, including:

- Pictures and maps (e.g., Google Earth, Google images, IntelliEarth)
- Search engines and news sites
- Business and government databases
- AIS aggregation sites
- Port databases (e.g., FleetMon)
- Contract sites (e.g., GovTribe, GovWin)
- Ship, port, and shipping line Web and social media sites (including Wikipedia)
- Google Dorking to find personnel and e-mail addresses

As far back as 2004, the IMO recognized that “the publication on the world-wide web [sic] or elsewhere of AIS data transmitted by ships could be detrimental to the safety and security of ships and port facilities.” Mariners and marine facilities should consider carefully the information that companies, vessels, and individuals post online. OSINT needs to be taken seriously, as it is very possible to infer sensitive or classified information from even a few items of unclassified/open source information.

Intellectual Property Theft

Intellectual property (IP) theft—aka IP piracy, economic espionage, and industrial espionage—are significant threats to any organization in any industry. IP theft means to rob a person or a company of their ideas, creative works, and inventions, including trade secrets, proprietary products or processes, patents, music, works of art, movies, and software. IP theft costs U.S. businesses more than \$600 billion annually; it is difficult to accurately estimate the impact on the global economy but it easily tops \$2 trillion.

While many countries have weak IP protections, China appears to be a particular purveyor of IP theft. The maritime industry has not escaped the attention of Chinese Bad Actors. In early 2019, reports surfaced that China-based hackers targeted 27 universities in order to steal maritime technology secrets and to obtain access to maritime military research. The targeted universities were primarily in Canada, Southeast Asia, and the U.S., and included Duke University, Massachusetts Institute of Technology, Pennsylvania State University, and University of Hawaii. The attacks used spearphishing e-mails that appeared to come from partnered universities. Malicious payloads included malware that was later used to move around the compromised networks and steal files related to maritime technology and research.

At around the same time, other sources reported that Chinese government hackers were targeting the U.S. Navy and industry associates, defense contractors, and partner research universities. The result of these attacks were successful exfiltration of military secrets, building China’s military capabilities at the expense of the U.S. In one example, hackers stole Navy undersea-warfare program data from an unidentified contractor, including the plans for a new supersonic anti-ship missile. An internal Navy review found that Iran, Russia, and others are also engaged in this activity against the U.S. Navy.

China is a maritime port superpower. Five of the 10 busiest container ports in the world are in China, plus another in Hong Kong. China also operates, or has a presence at, dozens of ports around the world, in countries that include Djibouti, France, Germany, Greece, Holland, Israel, Italy, Japan, South Korea, Spain, Sri Lanka, U.K., and the U.S. By 2017, China had some level of investment at nearly 30 of the top 50 container ports in the world, triple the number it had in 2010.

Because Chinese businesses are required to cooperate with their country’s intelligence agencies, there are legitimate concerns that Chinese port companies could be spying on commercial ships and military vessels from other nations, gathering critical information about the capability of these vessels, and possibly stealing other intellectual property. This access could also be a potential threat to the ports’ host countries and alliances such as the North Atlantic Treaty Organization (NATO). China has also financed, built, and maintained ownership of many ports around the world. As an example, the China Overseas Port Holding Company operates Pakistan’s Gwadar Port, located on the Arabian Sea. Gwadar is the world’s deepest seaport and has significant strategic importance because of its location on major fuel sea lanes. Their presence at ports around the globe also gives China’s Navy access to additional maritime facilities. Indeed, in 2021 alone, China was awarded a 25-year contract to operate the Port of Haifa and was found to be building a secret military facility inside of a port near Abu Dhabi.

Conclusion and Summary

This chapter has presented a wide array of case studies related to cyberattacks against elements of the maritime industry. This is a non-exhaustive list but, hopefully, sufficient to demonstrate that “theoretical” cyber vulnerabilities have moved beyond the merely possible and are now real—and have real-life impacts and

consequences, including tangible financial loss. And while serious, these attacks will become increasingly sophisticated and impactful over time, as new technologies such as artificial intelligence (AI) and IoT devices become more widely deployed.

The next chapter introduces port cybersecurity, the unique role that ports have in the maritime ecosystem, and some additional cyber case studies.

Chapter 4: Ports and Cybersecurity

Introduction

While the last chapter presented a set of cyberattacks on the greater maritime industry, this chapter focuses exclusively on cybersecurity related to ports. Ports are a microcosm of the entire MTS. There is a relevant adage to this topic: “If you’ve seen one port, you’ve seen one port.”^[13] While all ports are similar at a very high level—they are the interface between ships and the land—they all differ in the details. Any given port might include different combinations of many elements, including:

- military, government, commercial, merchant, and recreational vessels;
- ship owners and operators;
- shipping agents;
- cargo managers;
- intermodal carriers;
- port operators;
- marketing, and communications;
- infrastructure and operations technology management;
- port authorities;
- harbormasters, pilots, and traffic management;
- military security and civilian law enforcement;
- customs and immigration services;
- repair and maintenance facilities;
- terminals; safety and environmental inspectors;
- stevedores and other dock workers; and
- logistics and support companies and personnel.

Ports are not only integral parts of the maritime environment, they are standalone entities that serve as both a supplier and a consumer of services. In short, every type of cyberattack that can affect any part of the MTS is present at a port. It’s no wonder that they are such high-profile targets for would-be cyber intruders.



Figure 4.1. Port components at risk of cyberintrusion.

Port Components and Communication Flows

There are myriad functions, agencies, organizations, and people at a port. The breadth of the cybersecurity challenge is due to the many different components at a port that must be protected from cyberthreats and attacks on information (Figure 4.1).

1. The *terminal gate* serves as the secure entry point and is a component of the physical perimeter of the port. Computers and communications networks are key to the operation of security systems

that closely monitor the perimeter, from alarms and closed-circuit television (CCTV) to access control protections and traffic management systems. The gate also represents the handoff point for passengers, employees, cargo, and supplies (for both the port and the ships), and for access between the intermodal transport carriers (i.e., cars, trucks, buses, railroad, and airplanes) and the port itself. Any disruption at the perimeter can cause congestion or closure of the port facilities.

2. The *terminal* represents all information and communications technology (ICT) systems at the port. Think of *terminal* broadly; this can be the workplace that houses all port and port authority administration, as well as the facility that tracks cargo, passengers, liquid/dry bulk materials, and automobiles and trucks. In many ways, the terminal bypasses perimeter security by allowing material (data) to enter and exit the port without passing through the main gate. Attacks on data are a primary cyberattack vector, where Bad Actors will compromise computer systems to access sensitive information related to clients, employees, ships, and cargo information. These types of attacks against data usually involve malware, phishing, or computer hacking; motivation can range from cybercrime and cyberactivism to cyberespionage and cyberwar.
3. Another type of cyberattack that can occur against the *terminal headquarters* involves the manipulation or destruction of data, or knocking an ICT system offline. In either of these cases, the data can become unreliable or unavailable. Cyberattacks such as ransomware or denial-of-service can disrupt operations within a facility, resulting in shutdowns that can last for days.
4. *Industrial control systems (ICS)* and operational technology (OT) represent the cyber-physical systems at ports and on ships. With ICS/OT, computers interact with physical processes by direct, near-real-time monitoring and/or control of physical devices such as valves, pumps, cranes, propulsion systems, and cargo handling. If these systems are compromised, they can interrupt or shut down port operations, cause physical damage to equipment or cargo, or result in injuries to employees.
5. *Position, navigation, and timing (PNT)* refers to systems used for navigation and port logistics, such as AIS and GNSS. PNT systems are pervasive throughout the MTS, and are essential at ports for vessel traffic management and ships' situational awareness. Loss, disruption, or spoofing of PNT services can impact both vessel movements and the complex logistics systems at port facilities.
6. Vessels are, of course, the *raison d'être* of ports. Modern ships are floating computer networks; functionally, they include ships picking up and delivering cargo and/or passengers, port-owned boats that assist in the movement of larger commercial vessels (e.g., tugs and pilot boats) as well as workboats, safety vessels, and private or small commercial vessels transiting the area. A shipboard computer network compromised by a cyberattack could go on to infect other ships' networks or landside systems. Conversely, a successful cyberinfection at a port can compromise shipboard systems. Interconnectivity—sanctioned, rogue, or nefarious—between ships at dock and land-based maritime facilities occurs when Wi-Fi networks, USB storage devices, individual crew and port staff members' mobile devices, and more are shared without regard for security considerations.

While the components of a port are important in order to understand where cyberattacks might be targeted, it is illustrative to see how data flows between the many entities that have a presence at a port. Figure 4.2 shows a high level, generic view of these flows. The *port systems* block in the middle is meant to represent the various computer and information systems at a port. The other blocks represent information systems that interact in some way with the port systems. The diagram also shows that the different information flows exist due to different requirements or purposes, such as regulatory demands, financial transactions, or movement of routine operational data. As you look at the diagram, do not be concerned that every information subsystem and flow has not been properly identified; the point is to understand how complex the information requirements are and start thinking about the many possible vectors for cyberattack—and to develop a strategy against them.

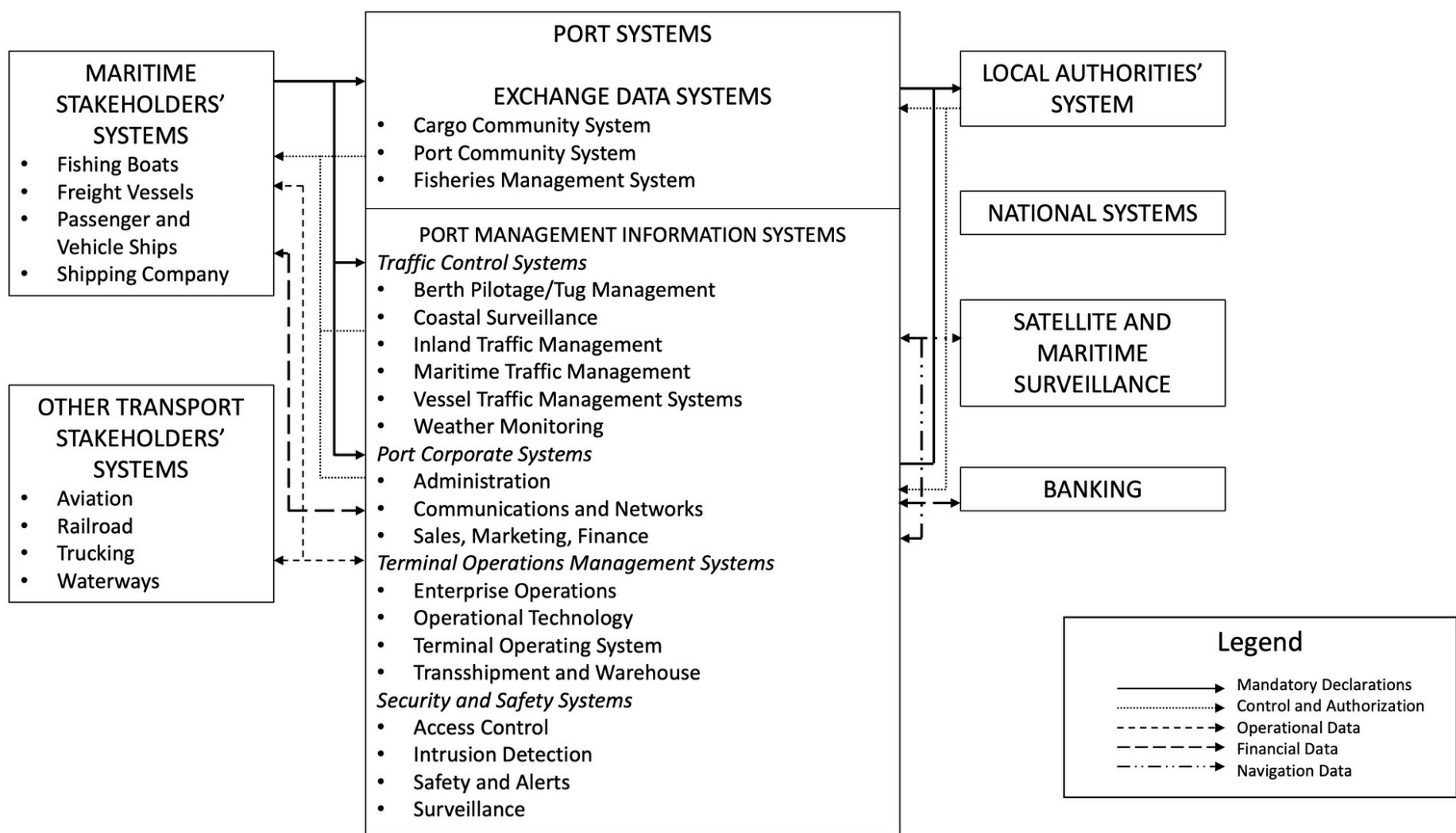


Figure 4.2. Data flows at a port.

The issues discussed so far may seem academic, but there is a very real consequence if they are ignored. A 2019 report by Lloyd's of London, the Cambridge Centre for Risk Studies, and Nanyang Technological University describes a hypothetical cyber intrusion on major ports across the Asia Pacific region. The so-called "Shen attack" was based on an extreme, but plausible, scenario in which malware carried by ships infected 15 ports. A virus jumped from one ship's network to the ports' cargo database, where records were modified or deleted, and the ports suffered a severe disruption in operations. Other ships were, in turn, infected with the virus after connecting to the ports' network. The economic losses from this scenario were estimated to be as high as \$110 billion, 92% of which is not covered by insurance. And while this was indeed a hypothetical scenario, an attack of this scale might not be that difficult to carry out. Because of the interconnectivity of the maritime supply chain, an incident such as this would cause significant economic damage to myriad business sectors around the world, including all forms of transportation, aviation, aerospace, manufacturing, and retail. Although the scenario had all attacks occurring at ports in Asia, productivity losses due to bilateral trade agreements led to indirect but significant economic losses in Europe and North America.

The bottom line is this: computer networks and international trade have made the world a smaller place. The global economy is not prepared for such an attack, and the MTS is the linchpin of the world's trade.

Ports and the Supply Chain

The importance of ports in the global supply chain cannot be over-emphasized. Today's supply chain is an incredibly complex, globally interconnected system with, by design, layer upon layer of outsourcing and integration. This results in a fragile ecosystem fraught with vulnerabilities.

MARITIME SUPPLY CHAINS: AMERICA'S PRIMARY LINK TO THE GLOBAL MARKETPLACE

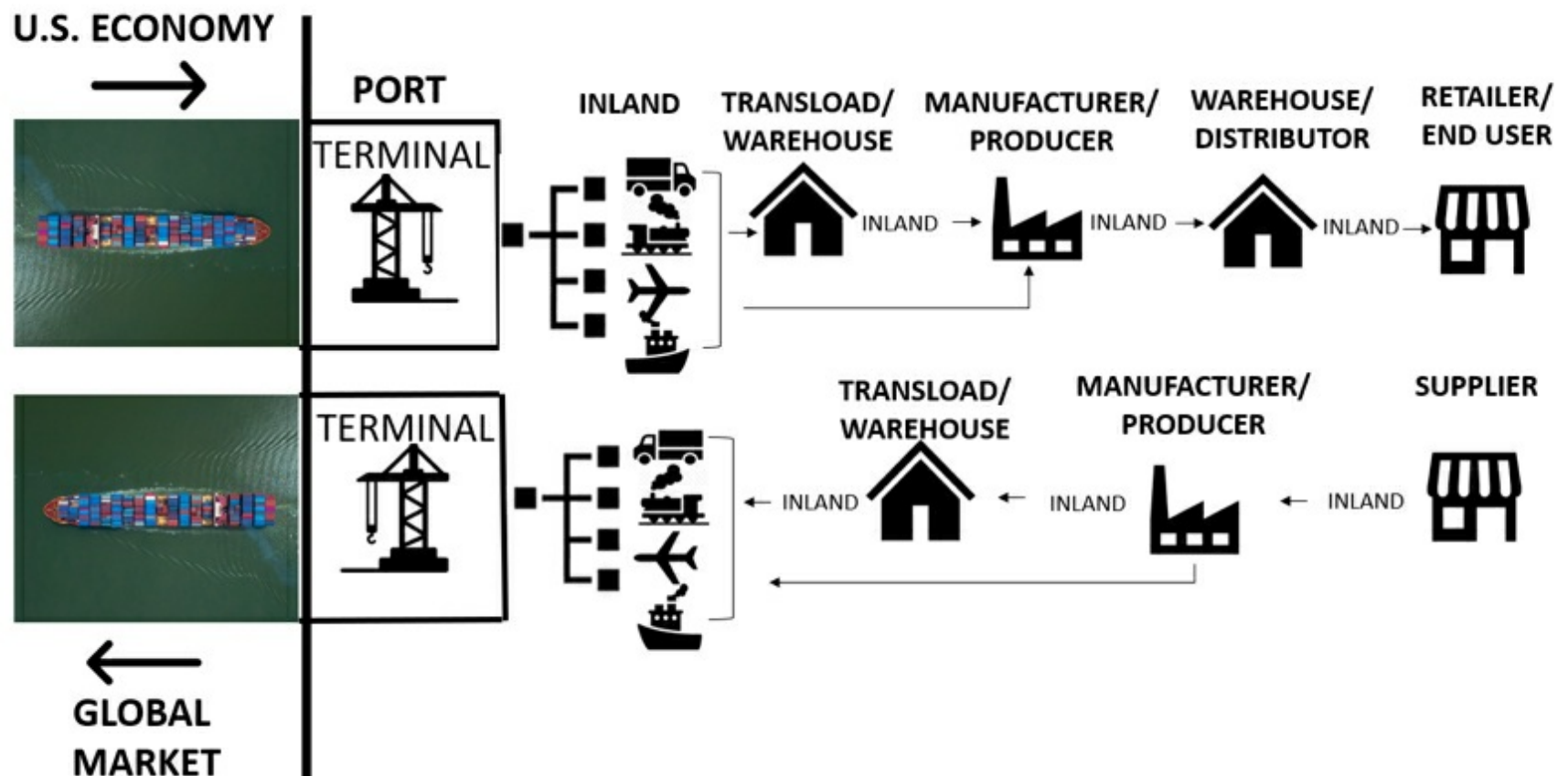


Figure 4.3. The maritime supply chain.

Figure 4.3 shows a simplified model of the supply chain. In its most elementary form, the supply chain includes two parties, namely, the *manufacturer* of a product and the *shopper*, or consumer of the product. Of course, there are several other steps in the process and the implied linearity in the figure is for illustration only.

The manufacturer must collect all the pieces and raw materials for its product from a variety of *suppliers*. In the strictest sense, there is actually another supply chain between supplier and manufacturer; if even one supplier cannot provide necessary raw materials to the manufacturer when they are needed, the manufacturer cannot build its goods and will be shut down, causing a ripple effect. It is this non-linearity that leads some to refer to the global supply chain as a hyperchain.

Once the manufacturer has built its product, it must move it to the market where consumers can find it. This is where *distribution* partners, notably in the transportation sector, come into play. The distribution can be as simple as a truck hauling fruits and vegetables to a local farmers' market, or as complex as vans taking products to an airport to be flown to a port to be shipped tens of thousands of miles away, to be then transported by rail to a final destination. Generally speaking, products are delivered to *retailers* where consumers buy the products, but Internet-enabled electronic commerce now short-circuits the retail process, so that the manufacturer is also an online store rather than a physical bricks-and-mortar facility. Even in this latter case, however, the transportation sector plays a role in the distribution of products.

The supply chain itself requires the movement of three things. First, *product*, which includes the raw materials with which to make things, sub-components which can be assembled into larger systems, and finished products to be delivered to consumers. Second, *information*, which includes product specifications, blueprints, orders, invoices, bills of lading, schedules, website order processing and tracking, standards, and much more. Last, but certainly not least, are *finances*: purchases, sales, distribution, payments, and all segments of the supply chain depend upon the exchange of currency.

Ports have a place at many points in the international supply chain. They are a supplier of services, distributor, and consumer, as well as the intermediate point in millions of other products' supply chains. As such, they are an attractive target for malicious actors, because suppliers, trade partners, shipping lines, and other organizations co-located at a port often have bona fide credentials that allow them to directly connect to systems behind firewalls and other cyber protections. If a Bad Actor wants to access a particular organization's information systems and cannot get through the target's cyber defenses, an alternative approach is to compromise a supply chain partner's network and use that access to penetrate the intended victim's system. The problem is exacerbated by the difficulty in enforcing security requirements with suppliers and partners in another country.

The U.S. government reported that supply chain cyberattacks rose 78% in 2018 compared to the previous year and European sources estimated a 400% growth in supply chain cyberattacks in 2021 compared to 2020. Both of these statistics underscore the growing importance of strong supply chain security. Increasingly, attacks on the supply chain target people and machinery. As the volume of machine-to-machine (M2M) communication between ships,

cargo and freight handlers, railroads, trucks, port operators, and customers grows, the entire supply chain is put at risk. As suggested above, even if truckers, for example, are not the direct target of a cyberattack, they could sustain residual damage by an attack elsewhere in the supply chain or a railroad network's vulnerability could be exploited to attack a port's network.

One of the most significant supply chain attacks in recent memory targeted SolarWinds, a U.S. software company. SolarWinds' Orion software provides enterprise network and supply chain management, and is used to monitor and manage both hosted and on-premises IT systems and network infrastructures. Used by 33,000 public and private sector customers, Orion is commonly configured with pervasive privileges, yielding extraordinary system-wide access.

Two APT attacks on Orion software were reported in December 2020. The first, SUNBURST, was conducted by a Russian hacker group called APT29 (Cozy Bear). The SUNBURST malware was inserted into the Orion code via a compromised certificate and backdoor in the software. The malware was then distributed to more than 18,000 customers at the next software update, with victims including AstraZeneca, DHS, FireEye, General Communications Headquarters (GCHQ), NATO, and NIST. It took SolarWinds an entire week to revoke the compromised certificate. The second attack, SUPERNOVA, was a supply chain attack implementing a remote access tool. This stealthy attack was likely performed by a second attacker. It is noteworthy that roughly a third of all victims of this cyberattack were not actual users of SolarWinds software, but downstream partners, once again illustrating that an indirect attack can be just as damaging as a head-on cyberassault.

Two incidents in 2021 showed the world the importance of maritime to the worldwide supply chain. Even though neither were cybersecurity incidents, they are harbingers of what could happen in a cyberattack.

The first event occurred when M/V EVER GIVEN became stuck in the Suez Canal in March. One of the largest container ships in the world, the 1,312 foot (400 m) EVER GIVEN has a capacity of 20,124 twenty-foot equivalent units (TEUs). EVER GIVEN was stuck in the canal for six days, with the cause attributed to 30-knot winds, the ship's speed, and issues with the ship's rudder size and alignment. More than 10% of global trade, including seven percent of the world's oil, passes through the canal every year, and the blockage cost upwards of \$9 billion a day. Shipping lines had to determine what to do with their vessels that were now in a queue waiting to see how long it would take to get traffic moving again; the alternate southern route would require a ship to transit the Cape of Good Hope, adding 12 days to the trip plus additional fuel, personnel, and transport delay costs. Although stuck in the mud for less than a week, EVER GIVEN was held in Great Bitter Lake by the Suez Canal Authority (SCA) until \$550M salvage costs and lost revenue fees were recovered. EVER GIVEN was finally released in July.

A second acute reminder of the impact of shipping on the supply chain are the backlogs at the Ports of Long Beach and Los Angeles, primarily due to a confluence of factors resulting from the impact of the COVID-19 pandemic. Due to slowdowns in manufacturing and shipping during the spring and summer of 2020, a sudden growth in shipments late in the year surprised and overwhelmed the ability to move goods. Extra ships arrived at the Ports of Long Beach and Los Angeles—the portal for nearly 40% of U.S. imports and exports—while they were operating at reduced capacity and efficiency. The ensuing bottleneck resulted from a combination of antiquated infrastructure, containers in the wrong place, and labor shortages related to the pandemic.

By February 2021, 177 container ships and more than 800,000 TEUs arrived at the two ports, a 31% increase in ships and 49% increase in containers compared to February 2020. In November 2021, a record 179 ships were waiting offshore to unload. Only part of the problem was with the ports' capacity to unload and store cargo; it was also aggravated by related capacity issues with the rail and truck carriers, and a global shortage of empty TEUs. By September 2021, the dwell time—the number of days that a container remains at the port after being unloaded from a ship—was nearly eight days on average if waiting for a truck and five-and-a-half days on average if moved by rail. Ports are not designed for long-term storage of containers; to clear the backlog, the ports considered charging carriers a fee if containers languished too long.

Product shortages due to hiccups in the supply chain's movement of goods also shows the fragility of just-in-time inventory schemes and the elimination of many warehouses in the manufacturing chain. While neither of the scenarios above was due to a cyberattack, they certainly indicate how attractive a target the supply chain can be to a cyberattacker. Indeed, there were many problems at ports due to unabated cyberattacks during the COVID-19 era, as will be discussed below.

Ports and Security

Over the decades, and particularly since the terrorist attacks of 9/11, ports have implemented stringent physical security processes. But there remains a disconnect between the emphasis placed by management and regulators on physical security versus cybersecurity.

Consider, for example, the U.S. Maritime Security (MARSEC) program, which allows the USCG and maritime industry partners to implement pre-planned responses to credible threats on maritime assets. The MARSEC threat levels and response plans, however, address physical threats, not cyberthreats. Some emerging cyber regulations focus on operational technology, but the overwhelming majority of attack vectors employ information technology. Although OT and IT are converging, most port security managers come from a world of physical security, and most ports do not have a Chief Information Security Officer (CISO).

Several port authorities have proactively responded to cyberthreats. As an example, the Port of Los Angeles became, in 2014, the first U.S. port to open a Cyber Security Operations Center (CSOC). The CSOC is certified as compliant with the International Organization for Standardization (ISO) 27001 information security standard. In early 2019, the port proposed a Cyber Resilience Center, signed a contract with IBM in late 2020, and officially opened in early 2022. This second-generation maritime cyber facility is intended to provide threat detection, attack analysis, information sharing, and threat response strategies amongst its stakeholders, including ocean carriers, terminal operators, freight and cargo haulers, and others in the maritime supply chain.

In May 2019, the Maritime and Port Authority (MPA) in Singapore opened its Maritime Cybersecurity Operations Centre (MSOC). The Centre's objective is to provide early detection, monitoring, analysis and response to potential cyberattacks on maritime critical information infrastructures. The Republic of Singapore Navy also hosts a regional Information Fusion Centre (IFC). Formed in 2009, the IFC brings together representatives from more than two dozen nations, monitoring maritime security events ranging from smuggling and piracy to human trafficking and illegal fishing. Cybersecurity was added as a sector of interest in 2020.

Case Studies: Ports and Cybersecurity

Cybercriminals and Ports

One of the earliest cyberattacks on a port reportedly occurred in 2012, when hackers for a crime syndicate broke into a cargo management system run by the Australian Customs and Border Protection Service. The criminal organization was transporting contraband goods in cargo containers mixed with legitimate cargo. The criminals monitored the containers' status in the system; if any were flagged as suspicious or warranting further investigation by customs authorities, the criminals would know, and simply abandon them.

From 2011-2013, the Port of Antwerp, in Belgium, was compromised by cybercriminals working with drug and arms smugglers. In this case, the smugglers recruited hackers to break into the port's computers. The hackers succeeded by using standard cyberattack methods: social engineering, physical access to network devices, and use of snooping devices (e.g., keystroke loggers). The compromised computer systems were those that controlled the movement and monitored the location of shipping containers. As in the case above, smugglers were shipping cocaine, heroin, weapons, and other illegal items packaged in TEUs containing legitimate cargo. The drug traffickers stole the containers with contraband goods by sending trucks with bogus bills of lading to the port, well before the real owner of the cargo knew that the shipment had arrived.

One of the other security vulnerabilities exploited by the smugglers was the use of a single-factor^[14] personal identification number (PIN); as long as the trucker provided a valid PIN, they could pick up a cargo container with no further proof that they were the authorized owner of the PIN.

In August 2021, the Port of Houston's Web server suffered a root-level intrusion by an unidentified state actor. The attack employed a Zero Day exploit of a critical vulnerability in the Zoho ManageEngine ADSelfService Plus service, used for self-service password management and single sign-on. The attackers were able to install malicious code on the server in order to obtain additional access, gain lateral movement, and steal user login credentials. Coast Guard Cyber Command (CGCYBER), CISA, and the FBI fielded a response team to assist the port in their response and recovery.

Social Engineering and Phishing

Figure 4.4 shows an e-mail that was received by a Payroll Department employee at a U.S. port. In response, the person who received the message sent W-2 tax information (including names, addresses, wages, and social security numbers) for 780 port employees to a bogus e-mail address for the Port Director. The e-mail recipient later advised the Port Director's secretary of the request, which triggered the port's incident response plan. Social engineering does not just fool inexperienced or naive people; this particular employee was experienced in payroll operations and had taken the port's cybersecurity training. In addition, this message was neither stopped nor flagged by the port network's e-mail spam and virus filters.

From: <Port Authority Director>
Sent: Tuesday, February 21, 2017 8:36 a.m.
To: <Employee in Payroll Dept.>
Subject: Call to Attention

Kindly send me the complete list of ALL employees W-2 wages and tax statements for the year 2016. It should be sent in PDF format, Kindly prepare and send me the list for a quick review.

Sent from my iPhone

Figure 4.4. Bogus e-mail sent to a port's payroll department.

Not all phishing campaigns result in a successful network breach. In 2018, a U.S. port marketing official was successfully phished, and the attacker was able to obtain their login credentials. In this case, however, an attempted financial attack was averted by quick action by the port authority's IT staff. The attacker was not done, however; more intense cyberattacks followed over the next three weeks with daily brute force login attempts around the clock. Investigators noted that the same source Internet Protocol (IP) addresses were seen more than 600 times per day. The attacks then spread to other users and departments at the port before the attacker gave up.

Some phishing attacks are sophisticated, using a two-pronged approach to create a more receptive environment for the actual attack e-mail. At one port, a voicemail was left during non-work hours at the finance office. The caller was friendly but urgent, identifying himself only with his first name and saying that he was from Maersk Line; among the phrases in the message were "second time I am leaving a voicemail," "need to make the payment on-time," and "e-mail to Accounts Receivable will be forthcoming." The message also said that the recipient could call back, but the caller gave no last name, phone number, or e-mail address. This appears to be a carefully crafted script, leaving the voicemail as a way to make a subsequent spearphishing e-mail appear more plausible.

Cyberattacks and Ransomware

In early 2018, the FBI notified the Port of Longview, on the Columbia River in Washington, that it had been victimized by a cyberattack. In this case, the port did not detect the intrusion, but evidence of the compromise was found by the FBI as part of a larger, separate investigation. This compromise affected personnel information for 370 past and current employees, as well as 47 vendors. The Port of Longview had formerly managed the nearby Port of Kalama employee benefits program, and the latter port's employee information was also compromised. This attack was linked to IP addresses associated with service providers in Kazakhstan, Liberia, and Russia.

Multiple ports were hit by ransomware attacks in September 2018. The first was against the Port de Barcelona. Few details of the cyberattack were released, but it is believed that several servers in the port's security infrastructure were breached although, reportedly, there was no impact on maritime operations. It has been suspected, but not confirmed, that the port was struck by ransomware. A week later, the Port of San Diego was hit by the SamSam ransomware with a demand for a Bitcoin payment. The attack affected more than 500 workers, and disrupted computer systems, business services, public records requests, and Harbor Police operations. The attack was followed by attempted exploits of Microsoft's Remote Desktop Protocol (RDP) vulnerabilities. Later in 2018, a pair of Iranian hackers were indicted by the U.S. Department of Justice for developing SamSam, although there have been no forthcoming arrests.

In November 2020, the Port of Kennewick, located on the Columbia River in Washington, was struck by ransomware. The attack bypassed firewalls and anti-malware software to lock system administrators out of their systems. The perpetrators demanded a \$200,000 ransom; all port services were down for several days as servers were re-built from offline backups.

Transnet, the South African port, rail, and pipeline operator, was subjected to a ransomware attack in July 2021. More than one terabyte (TB) of Transnet's corporate files, including PII and financial records, were encrypted with the Death Kitty ransomware. The Terminal Operating System (TOS) at the Ports of Cape Town and Durban—the two busiest sub-Saharan African shipping terminals—were compromised, disrupting container operations and making the company's website inaccessible for several days. Transnet declared *force majeure* for nearly one week to financially protect itself.

Ports in Cyberwar

Militaries around the world have historically defined three domains of war: air, land, and sea. In recent years, space and cyberspace have emerged as new domains of conflict between nation-states. One of the terms we often hear today is *cyberwar*, which is controversial because it is surprisingly difficult to define and codify. While the *Tallinn Manual*^[15] provides an academic review of how international law applies to cyber conflicts, it is a non-binding

study and there remains no internationally agreed-upon definition. Suffice it to say that cyberwar includes attacks occurring in cyberspace between nation-states, with the intent to further each country's strategic goals. Any kinetic military action (i.e., one taking place in one of the other domains) can involve attacks in cyberspace, although cyberwar can presumably exist purely in the cyber domain.

As cyberwars escalate, it is inevitable that ports become targets. In April 2020, Iran attempted a cyberattack on Israel's water command and control infrastructure. The attack was launched via servers located in the U.S. and occurred over a two-day period. Only minor damage and disruption in service was sustained by the water system.

In response, Israel launched a cyberattack on Shahid Rajaei Port the following month. The newest of two major shipping terminals in Bandar Abbas on the Strait of Hormuz, the Port handles 100 million tons of cargo annually and has 40 cargo berths. The cyberattack caused minimal damage but was hugely disruptive to port activities. Computers regulating the movement of vessels, trucks, and cargo were taken down and all port traffic came to a sudden halt. The resulting massive traffic jams on the roadways and waterways lasted for several days.

Another cyberattack targeting Iranian government institutions occurred in October 2020. This attack affected the electronic infrastructure of the country's ports. Few details are known about this attack and no one has claimed responsibility.

Cyberwar by adversarial nations is hardly new, and cyberattacks on non-military targets is also not new. In 2018, the FBI and DHS reported that Russian government hackers have targeted government entities and U.S. critical infrastructure sectors—including ports—since at least 2016. The cyberattack methods employ standard hacking attack vectors, including:

- Spearphishing e-mails (from a compromised legitimate account)
- Watering hole domains
- Credential gathering schemes
- Open-source and network reconnaissance
- Host-based exploitation
- Targeting industrial control system and operational technology infrastructures

The attackers initially exploited trusted third parties (e.g., supply chain partners with weaker security) and used these sites to stage attacks on the intended victims.

Regulatory Guidance for Port Cybersecurity

Regulatory guidelines related to cybersecurity in the global MTS are discussed in detail in Chapter 8. Given the unique nature of ports, this section introduces regulations specifically related to port cybersecurity. Several organizations provide guidance for cyberdefense related to ports, including the European Union Agency for Cybersecurity (ENISA), the Institution of Engineering and Technology (IET), and the International Association of Ports and Harbors (IAPH). These will be discussed in detail in Chapter 8. Suffice it to say that port cybersecurity is the subject of significant regulatory mandates.

In March 2020, USCG released Navigation and Vessel Inspection Circular (NVIC) 01-20, titled *Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities*. This rule asserted that cybersecurity is, in fact, included under the Maritime Transportation Security Act (MTSA) of 2002. NVIC 01-20 requires facilities to assess and document computer system and network vulnerabilities in a Facility Security Assessment (FSA), and address all identified vulnerabilities in applicable sections of the Facility Security Plan (FSP). In addition, the FSP cyber amendments or annexes were to be submitted to the local COTP by October 2021.

Conclusion and Summary

This chapter has presented some of the ways in which ports are at risk from cyberattack. As stated earlier, they are a microcosm of the MTS; any vulnerability in any segment of the MTS can be found at a port.

The next chapter continues to explore maritime cybersecurity, with a discussion of shipboard networks and communications systems.

Chapter 5: Shipboard Networks and Communications Systems

Introduction

A ship is a floating city and, as such, is a floating information and communications technology (ICT) platform. Vessels today increasingly rely on networks for communication between people, between shipboard systems, and for human control of shipboard systems. External networks are used for official and unofficial communications, regulatory and administrative functions, and ship-to-ship and ship-to-shore conversations. This chapter discusses some of the shipboard communications networks and describe some of their cyber vulnerabilities.

Shipboard ICT Overview

There are a variety of communications networks to which a ship must subscribe for routine or specialized operations (Figure 5.1). Some external networks are private, relatively secure, and might or might not use encryption; public networks are totally open to anyone with a receiver. External communications networks include:

- *Maritime very high frequency (VHF) radio*, routine on every vessel of any size, as well as a large number of smaller commercial, fishing, and recreational boats. Channel 16 (156.8 MHz) is the international hailing and distress frequency.
- *Vessel monitoring systems (VMS)* allow environmental and fisheries regulatory organizations to track and monitor the activities of fishing vessels.
- *Long Range Identification and Tracking (LRIT)* communications is present on all passenger and cargo ships, and on mobile offshore drilling units to report their position every six hours. LRIT reports are generally made over the ship's satellite communications network, and are private and secure.
- *Virtual private networks (VPNs)* allow private, secure communications between the ship and another party, using the Internet and other data networks. Voice over Internet Protocol (VoIP) solutions allow VPNs to be used for either voice or data communications.
- *Very Small Aperture Terminal (VSAT)* systems allow two-way communication with satellite ground stations via a satellite provider, generally for data communications.
- *Global satellite communication providers* such as Globalstar, Inmarsat, and Iridium, operate constellations for mobile and fixed telephone and data communications services for maritime, aviation, and other mobile sectors. SpaceX's nascent StarLink service is just now coming online in this arena; when fully deployed, this system alone could have as many as 42,000 small low Earth orbit (LEOS) satellites with which to offer high-speed broadband for voice and data services.
- *Intellian Fleet Broadband (FBB)* provides voice, data, text (SMS), and fax service via satellite.
- *Maritime cellular services*, such as Cellular at Sea, are becoming increasingly common onboard ships, providing seamless cell phone, data, and texting services using standard mobile phones and roaming capability.
- *GNSS and AIS* are designed for position, navigation, timing, and situational awareness. GNSS and AIS are the subject of the next chapter.

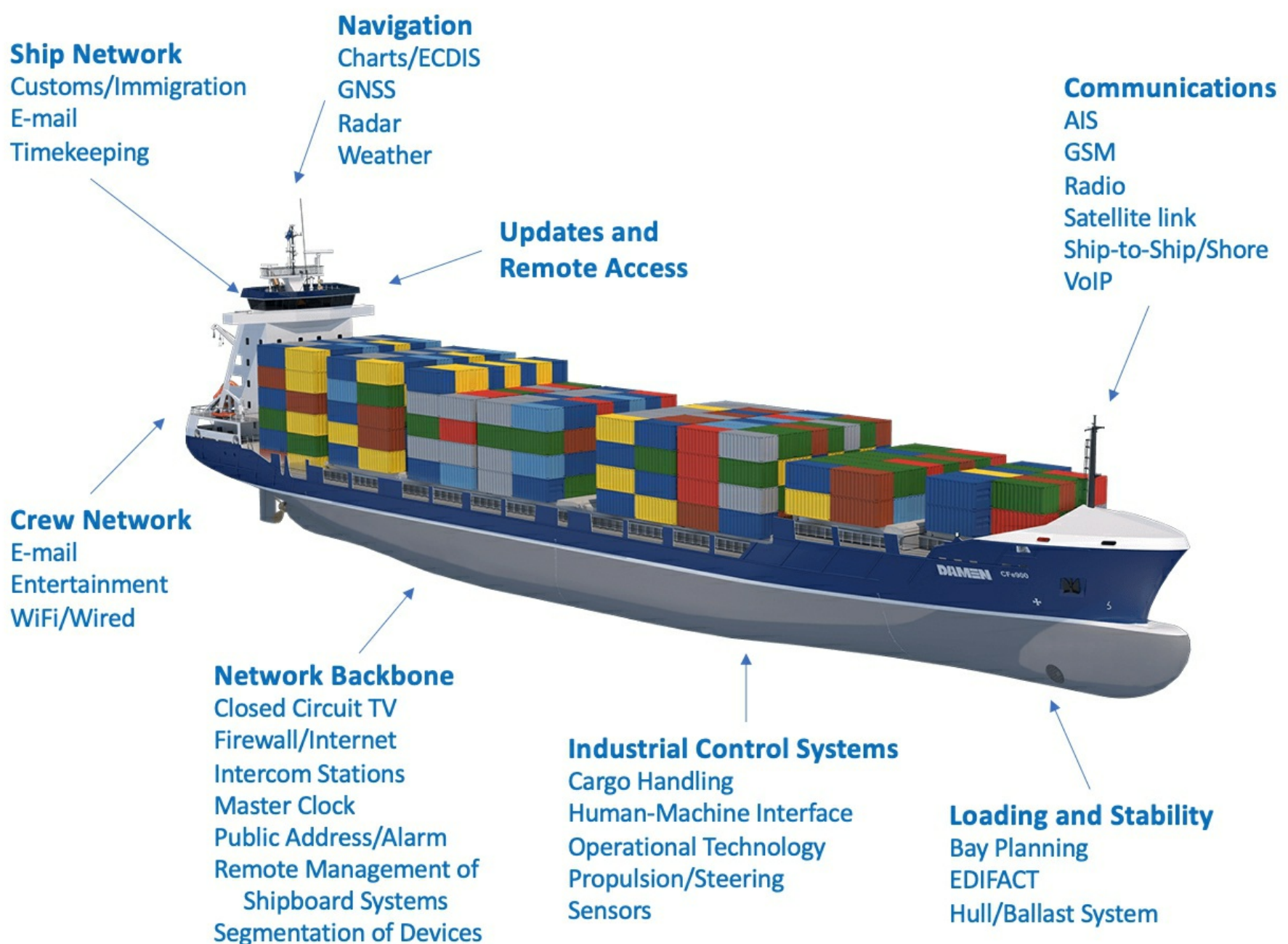


Figure 5.1. Networks aboard a ship.

Ships themselves have many systems interconnected by one form of communications network or another, such as:

- *Bridge Navigation Systems*, including AIS, Electronic Chart Display and Information System (ECDIS), GNSS, LRIT, and radar
- *External data and telecommunication systems*, such as FBB, Internet, VHF, and VSAT
- *Mechanical Systems*, such as the main engine, auxiliary engine, steering control, fire control, and ballast management
- *Ship Monitoring and Security Systems*, such as closed-circuit television (CCTV), Ship Security Alert System (SSAS), access control systems, sensors, public address systems, general alarms, intercoms, master clock, bilge control, freshwater plant, electrical power generation and distribution, and cooling water distribution
- *Cargo Handling Systems*, such as valve remote control systems, level/pressure monitoring systems, bay planning, stress monitoring, and Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT)

Some vessels also have their own specialized networks, such as Combat Command and Control Systems on warships, entertainment systems and point-of-sale (POS) networks on passenger vessels and cruise ships, and VMS on commercial fishing boats.

Within the skin of a ship, many of the most commonly used maritime communications protocols are rooted in the 1980s and not designed with security in mind. These protocols have their own security vulnerabilities, such as denial-of-service, frame injection and spoofing, eavesdropping, and man-in-the-middle attacks. In addition, the different shipboard networks are interconnected in unexpected ways and, therefore, it is sometimes possible to move laterally from one network to another, including from outside the ship. ^[16]

The remainder of the chapter examines some of these vulnerabilities and potential attack points in greater detail.

Cybersecurity and Shipboard Networks

This section examines and describes cyber vulnerabilities and some of the other related issues of the internal networks on board a ship.

Bridge Systems

Bridge systems are the command center of a ship. All onboard systems come together at the bridge, providing a mechanism for the master or crew to obtain situational awareness about all aspects of the vessel and its contents. Bridge systems remain vulnerable to hacking due, primarily, to poor security in the ship's communication protocols and network design, such as satellite communication terminals exposed on the Internet, administrative interfaces accessible by insecure protocols (e.g., Telnet^[17] and Hypertext Transfer Protocol [HTTP]), and because shipboard networks generally do not employ message authentication, encryption, or integrity checking. This is further exacerbated by poor security hygiene on the part of users who all-too-frequently employ easy-to-guess default login credentials (such as relying on a username of *bridge* and a password of *12345*), and poor password management—failing to change passwords frequently, for example, or choosing not to use two-factor authentication.

Maritime cybersecurity company Naval Dome performed a number of cyber penetration tests on ZIM GENEVOA in 2017. They reported three different types of successful cyberattacks, all performed without the cooperation of the ship's crew. The first vulnerability was related to the ECDIS. Using the ship's satellite link, attackers sent an e-mail with a malware attachment to the master's computer, which is regularly connected to ECDIS for routine chart updates. During the next chart update cycle, the virus moved to the ECDIS computer. The malware was specifically designed to alter the ship's position during the evening hours without changing the display; subtle changes were made to position, heading, depth, and speed information without anyone on the bridge noticing.

The second vulnerability was found in the radar system. This attack employed the Ethernet network switch that connected the radar, ECDIS, voyage data recorder (VDR), and bridge alert system networks. Malware was able to delete radar targets from the bridge radar display, effectively blinding the ship to nearby vessels. The system interface showed the radar to be working correctly, including all detection thresholds properly set so that the bridge officers had no reason to suspect a systemic failure.

The final breach occurred in the Machinery Control Systems (MCS). In this case, a virus was inserted into the MCS via an infected USB thumb drive found lying around by a crew member, who inserted the device directly into a networked computer. The virus ran automatically and moved to attack other auxiliary computer systems. The first target was the ballast system; valves and pumps were disrupted and stopped working, but the operator display showed normal operation. Other potential MCS auxiliary system targets included the air conditioning, generators, and fuel systems.

Engine Control Systems

Engine control systems monitor and control ship engines and propulsion systems. One widely used engine control system was found to have major security design flaws. In 2018, reports emerged that the Auto-Maskin DCU 210E RP 210E engine controller and Marine Pro Observer App had several authentication- and encryption-related vulnerabilities, namely, use of hard-coded credentials that could not be changed by users, the inability to authenticate the sending device, and the cleartext transmission of sensitive information. These flaws could allow an attacker to access the units and control connected engines, determine what sensors are present and in use, read or modify configuration information and other settings, and send arbitrary control information to the engine control units.

Ballast Systems

Ballast systems have been controlled by software and computer systems for decades. One of the more catastrophic maritime software failures occurred in the ballast control software of MS ZENOBIA. In 1980, ZENOBIA started listing to port during the first leg of her maiden voyage from Sweden to Syria. Righted after removing excess water in the ballast tanks, she continued on her voyage. At Larnaca, Cyprus, the listing reoccurred. The shifting ballast water was found to be due to a software error in the computerized pumping system. The ship was towed out of the harbor as a precaution. As ballast water continued to be shifted to one side, the ship came to a 45 degree list. After the port captain refused a request for her re-entry to the port, ZENOBIA capsized in 138 feet (42 m) of water.^[18] Although not a cyberattack, per se, this incident was a harbinger that automated systems can serve as an effective vector for harm.

Chris Roberts, a well-known cyber researcher who claims to have hacked into a variety of airplane and shipboard systems, made a presentation at the 2018 DEF CON hacker conference, during which he demonstrated the ability to remotely log in to a ship's network via the Internet by guessing usernames and passwords. He was then able to move laterally and gain access to the maintenance system network, at which point he was able to bring up the ballast control module. Although no nefarious action was taken, the demonstration of the capability was significant—and eye-opening.

In July 2021, a report describing a possible set of cyberattacks on ICS attributed to the Islamic Revolutionary

Guard's cyber unit, Shahid Kaveh, was publicly released. Attacks on ballast systems were one of the subjects of the report.

Cargo Loading and Balance

The importance of proper load balancing on a ship is obvious; an improperly balanced vessel is unstable and rough seas or shifting cargo can cause a ship to capsize. One notable example was M/V HOEGH OSAKA, a high-end car carrier that ran aground after leaving Southampton (U.K.) in 2015 and was stranded in The Solent off the Isle of Wight for 19 days. After leaving the port, the ship developed a 40-degree starboard list, leaving the rudder and propeller out of the water. A subsequent cargo shift resulted in a hull breach, allowing seawater to enter the vessel. The ship was very near a deep-water channel; had it sunk there, it would have blocked container ships, passenger ships, and ferries. It was later found that a "significant difference" between the actual and estimated cargo weight left HOEGH OSAKA unstable before leaving port and that the cargo was distributed so that upper vehicle decks were full while the lower vehicle decks were lightly loaded.

In a more recent, yet similar, episode, M/V GOLDEN RAY was grounded off the southeast coast of the U.S. in 2019. The 656 ft. (200 m) vehicle carrier, built in 2017, had 4,200 automobiles on board and began to list soon after leaving the Port of Brunswick, Georgia, most likely due to inaccurate stability calculations. The captain deliberately grounded GOLDEN RAY to keep her out of the shipping channel but, regardless, the port was closed for four days. No one was injured in this incident, but the vessel was a total loss. Removal of the vessel took more than two years.

An improperly loaded vessel can also capsize right at the dock. In early 2019, a 295 ft. (90 m) cargo ship capsized at the Shahid Rajaei Port in Iran. This accident was due to a "lack of coordination between the ship's officer and the contractor for loading and unloading." Several workers were injured during this incident.

In February 2021, the 13,100-TEU MAERSK EINDHOVEN lost power in heavy seas off the east coast of Japan. A loss of engine oil pressure triggered a safety feature that resulted in an automatic shutdown of the vessel's engine. Even though the incident lasted for only four minutes, the severe rolling of the 1,202 ft. (366 m) vessel resulted in the loss of 260 containers overboard and damage to another 65 containers.

None of these events were cyberattacks, but all clearly demonstrate the potential result to both ships and nearby ports when a cargo vessel becomes unstable. It also suggests a possible attack scenario. A Bad Actor could attach a low-cost, small-footprint computer—such as an Arduino or Raspberry Pi—onto a target vessel's network. By monitoring communications of other devices, the computer could monitor the vessel's pitch, roll, and yaw to determine when the ship is in heavy seas; it might also monitor the ship's latitude and longitude. At some pre-determined threshold, or even in response to an external signal, the computer could spoof an oil sensor, sending bogus *low pressure* indications, resulting in an engine shutdown. This combination of eavesdropping and man-in-the-middle attack is neither technically difficult nor expensive.

Cargo loading information is typically exchanged between the ship and port using standard United Nations (UN) Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) messages.^[19] Bayplan/Stowage Plan Occupied and Empty Locations (BAPLIE) and Verified Gross Mass (VERMAS) messages are commonly used to send information about the contents on a vessel, including the location of cargo containers. These messages are exchanged between many parties, including shipping agents, cargo centers, stevedores, and the ship's master.

In 2017, Pen Test Partners described the ease with which EDIFACT messages could be manipulated, due to the fact that there is no security associated with the messages or their transmission between interested parties. By manipulating BAPLIE and VERMAS messages, for example, an attacker could alter the weight value of containers so that load-planning software causes an unstable load (e.g., place heavy items high in the stack and light items lower in the stack), modify the flashpoint value of a flammable vapor so as to cause a dangerous storage scenario, change the reefer designation so that a refrigerated container is assigned to a non-powered bay, or change the designation of an odor-sensitive cargo (e.g., coffee) so that it is not in an odor-free location.

Other EDIFACT messages exchanged between trading partners can be manipulated to expedite theft of cargo and other cybercrimes. The Container Discharge/Loading Order (COPRAR) message, for example, contains the order to the cargo terminal that the specified containers are to put onto or taken off of a ship; cargo can be misdirected to an alternate port by manipulating these messages. The Container Gate-In/Gate-Out Report (CODECO) message confirms that the specified containers have been delivered to, or picked up by, the inland carrier, which can be manipulated further to facilitate theft of cargo at a port.

Pen Test Partners also described ways to attack a ship's hull stress monitoring system (HSMS), designed to ensure that the cargo load does not exceed the vessel's hull design specifications. HSMS sensors monitor the hull stress at port and at sea, sending alarms to the bridge and VDR if stress levels become dangerously high. The report showed

that HSMS hacks can disable these alarms so that an improper loading of a ship might go undetected, thus causing disaster at sea.

Shipboard Security Systems

Shipboard security systems have not been widely reported as suffering from cyberattack, but they are not immune. In 2018, a message on Twitter contained images that the sender claimed were from hacked cameras from the previous day before fishing vessel MIST arrived at Port of Dakhla in Morocco. While the photos matched the size and color of the vessel, the pictures themselves lacked metadata and an IP address, thus making it difficult to substantiate the claim.

What makes the scenario above plausible was a verified attack the previous year. A Louisiana-based maritime company reported that cameras on a quarter of its small fleet of boats had been compromised. In this case, hackers exploited a weakness in the camera's authentication procedures and accessed them remotely via the Web; the camera's contrast controls were set to darken the resolution, effectively blinding the camera. Other reports emerged that this same camera had previous issues in which remote users could circumvent authentication and 13 other vulnerabilities that dated back as far as 2013.

Types of Internet-connected cameras that can be remotely accessed and managed range from consumer-grade home security hardware to state-of-the-art industrial security and surveillance systems. Like all IoT devices, these so-called *smart cameras* are only as secure as the installer and system administrator make them, and even that is dependent upon how much user control the manufacturer builds into the devices. Hacked IoT devices organized into botnets have been used in some of the huge DDoS attacks discussed earlier in this book. It is imperative that any Internet-attached devices have their highest level of security activated to prevent them from being turned into tools for Bad Actors.

Voyage Data Recorders

A voyage data recorder, as the name implies, captures and records dynamic data related to a ship's voyage, including bridge conversations, VHF audio, radar, GNSS tracking information, speed, heading, depth, watertight and fire door status, alarms, wind direction and speed, and more. Although sometimes compared to an airplane's black box, any number of studies have shown that VDRs can be tampered with and modified by the vessel's crew or a hacker. One of the first VDRs shown to be susceptible to unauthorized access, modification, or deletion of data was the Furuno VR-3000 VDR in 2015.

These findings are significant. Not only is it possible for hackers to potentially modify data to cover up the evidence of criminal activity or the true location of an incident, it is also possible for crew members to modify VDR data. In early 2012, for example, marines aboard the Italian tanker M/V ENRICA LEXIE shot and killed two fishermen off the coast of India, claiming that they thought the fishermen to be pirates. The VDR data from the Italian ship was reportedly corrupted and, therefore, unavailable to investigators; Indian authorities suspected that the data had been destroyed on purpose. Later in 2012, Singapore-flagged cargo vessel M/V PRABHU DAYA was involved in a hit-and-run collision with a fishing boat, killing three fishermen. One of the ship's crew members reportedly hacked into the Furuno VR-3000 VDR and deleted what could have been incriminating data.

Cybersecurity and Communication Systems

This section examines cyber-related aspects of voice and data communication networks on board a ship.

Satellite Communications

Satellite communication (satcom) networks are essential for ship safety at sea, as well as connections to shore-based facilities for command, control, weather reports, chart updates, and more. A 2015 report demonstrated the ability to eavesdrop on, and insert data into, a Globalstar satellite system by exploiting a vulnerability in the STX3 transmitter chip. The STX3 does not encrypt data, allowing an attacker to build an inexpensive sniffer to read the data traffic. The researchers who reported this were able to read GPS coordinates and insert data into the stream.

The mention of the STX3 chip might seem a bit overly detailed for a high level treatment of this subject matter. The significance is not just in the vulnerability of the chip, however, but the fact that attackers can *find* the susceptible chip using online Internet databases. websites such as *censys.io* and *shodan.io* are but two of a handful of search engines that can be used to find a myriad of devices on the Internet, ranging from Webcams and smart refrigerators to systems with particular protocol vulnerabilities and specific hardware.

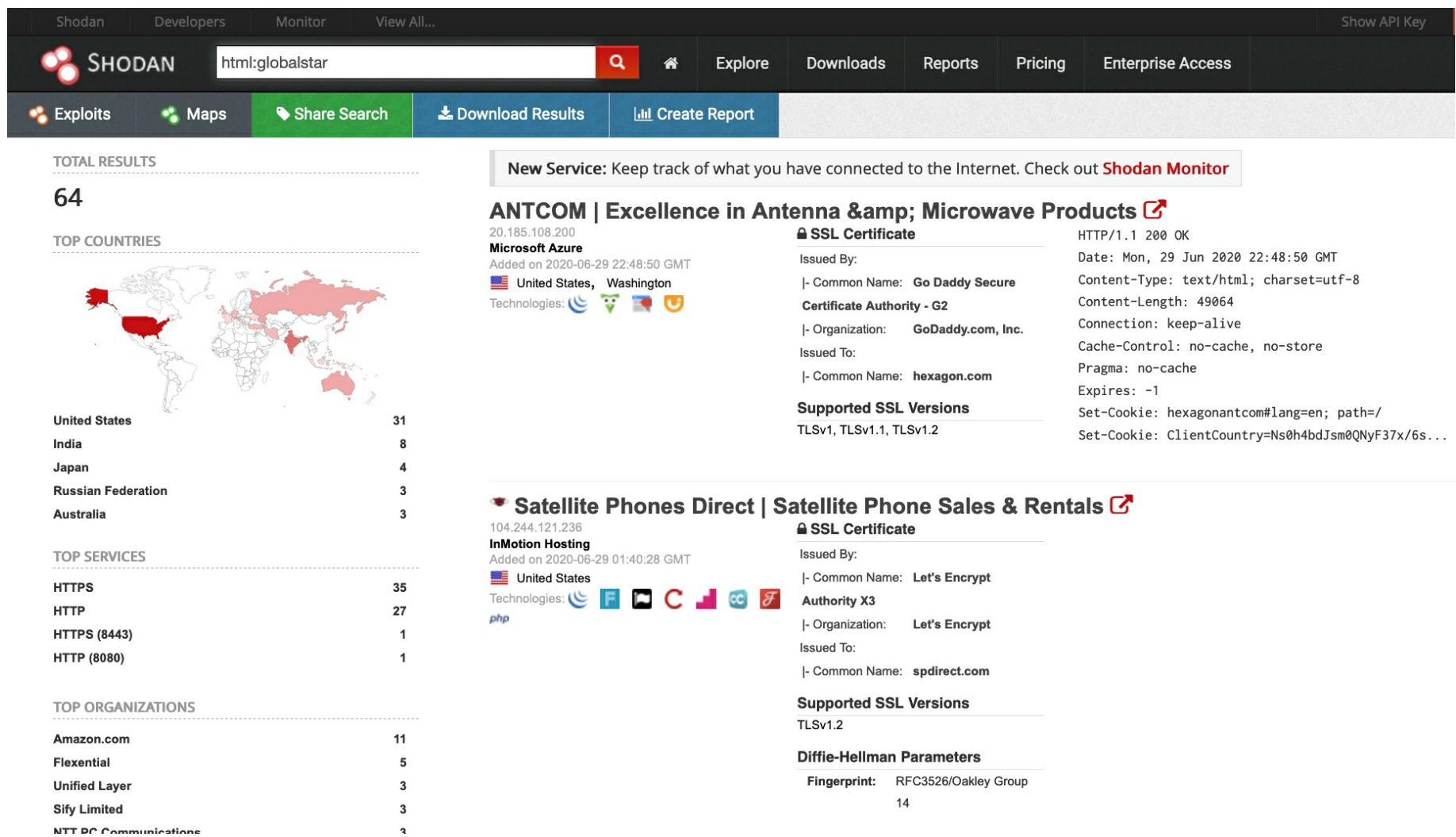


Figure 5.2. Results of a search for Globalstar devices on *shodan.io*.

Figure 5.2 shows such a search for Globalstar devices accessible via the HTML protocol, using the search string *html:globalstar*. Many of the devices found on Shodan continue to use their default username and password (e.g., *admin/1234*), so finding such devices on the Web gives a Bad Actor possible attack vectors.

Vulnerabilities in satellite communications systems have been reported at Black Hat hacker meetings as far back as 2014. Satcom devices were shown to be susceptible to remote attacks leading to both safety and security risks. The demonstrated vulnerabilities include system backdoors, insecure communications protocols, lack of input validation, and the ability of rogue applications to directly attack the device’s operating system. As a result, an attacker has the ability to:

- Disrupt, intercept, or modify onboard satellite communications;
- Attack crew members’ devices;
- Control satcom antenna positioning and transmissions;
- Perform high intensity radiated field (HIRF) cyber-physical attacks; and,
- Reverse engineer product backdoors to gain access.

Similar issues have been shown with VSAT systems connected to the Internet. There are many applications for VSAT on a ship, including updating electronic navigational charts (ENC), transmission of AIS messages, Voice-Over-IP communication, e-mail, and Internet searches.

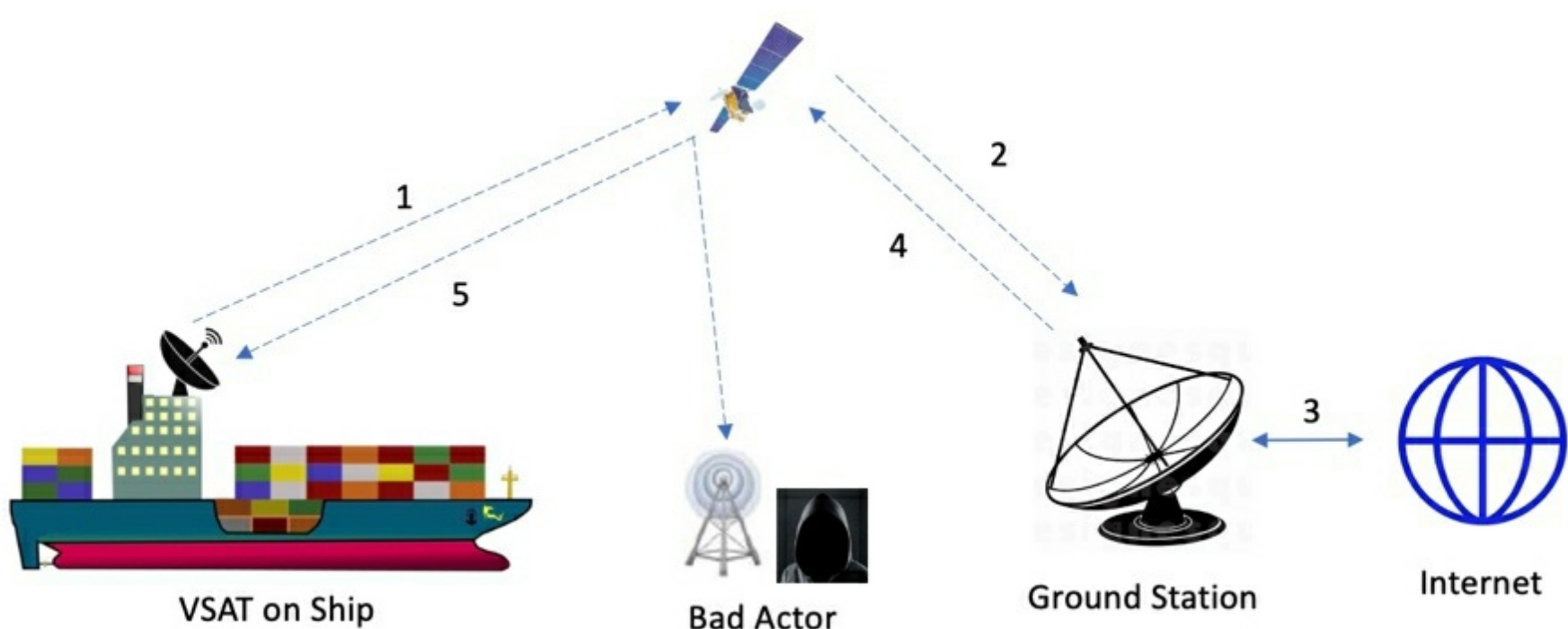


Figure 5.3. VSAT communications.

Figure 5.3 shows the pathway of the communications in a VSAT system. The VSAT uplink (1) on the ship sends data to the satellite that, in turn, transmits on the downlink (2) to the satellite provider's Internet Service Provider (ISP) (3). Traffic back from the Internet traverses the uplink (4) back to satellite. The transmission on the downlink (5) back to the ship is the vulnerable part of this transaction; the satellite's footprint covers a large geographical area on Earth's surface, which is why a Bad Actor can eavesdrop on this side of the conversation or hijack the Internet session.

In 2020, presentations at both Black Hat and DEF CON showed that insecure satellite Internet services potentially threaten vessel (and aircraft) safety. In one particular demonstration, a team from Oxford University intercepted signals from 18 satellites with airplane and ship Internet data in a 39 million square mile (101 million sq. km) area that included the Caribbean, China, India, and the U.S. The intercepted messages included:

- Communications from an Egyptian oil tanker reporting a malfunctioning alternator as the vessel entered port in Tunisia; the messages stated that the vessel would not be seaworthy for a month or more, and identified the name and passport number of the engineer sent to fix the problem
- A cruise ship broadcasting sensitive information about its Windows-based local area network, including the log-in information stored in the system's database
- An e-mail that a lawyer in Spain sent to a client about an upcoming case
- The account reset password for accessing the network of a Greek billionaire's yacht

Communications Platforms

AmosConnect™ is a maritime communications system that works with a ship's satellite equipment to integrate vessel and shore-based office applications and Internet access for the crew, e-mail, messaging, position reporting, weather reporting, and more. This system is usually deployed on a ship's IT network backbone, but should be separate from the navigation systems, Industrial Control Systems, and other networks. AmosConnect, a product of an Inmarsat subsidiary, is used on thousands of ships around the world.

Two vulnerabilities in AmosConnect version 8 (AC8) were reported in 2016. One was a flaw called an *SQL Inject*, which allows a nefarious user to enter bogus data in the login form and gain access to the system; the other was a built-in backdoor account with full system privileges. The flaws were reported to Inmarsat. In late 2016, Inmarsat notified users that AC8's end-of-life would be in mid-2017 and suggested that users downgrade to AmosConnect 7. A patch to AC8 was issued in early 2017 and the current AmosConnect software remains at version 7.

Shipboard Networks

Ships today employ wireless network access to the Internet for the same reason that shore-based facilities use it: ease of deployment, ease of connection, and high-speed access. And, shipboard Wi-Fi networks suffer from the same vulnerabilities as their shore-based counterparts. First, the network is vulnerable to unauthorized access unless it is using the strongest security. Second, personal or *ad hoc* access points put in place by crew or passengers are difficult to detect and may not be adequately secured, potentially weakening the security of the entire network. Third, unsecured Wi-Fi access points attached to control system and other shipboard networks, including entertainment systems and vendor POS terminals, can provide another vector for unauthorized access.

Even wired networks provide a vector for rogue users. Unused network jacks that are connected to a network switch allow anyone to plug in and gain access to the network backbone. One common attack vector is to find an unused jack in a wiring closet and hide a rogue wireless access point, giving an attacker undetected 24/7 access. Alternatively, an attacker can find any obscure active network jack and insert a hub; this allows the attacker to surreptitiously add a new network device or rogue wireless access point at any time, without disabling any current devices.

Finally, many public-facing networks are secured against users doing unauthorized activities from the graphical user interface (GUI) or Web browser, but are not protected from command line tools. In one case, public computers on a cruise ship limited users to applications accessible via the Windows GUI. It did not adequately protect, however, against a user opening the command line interface. Once they were at the DOS prompt, the user was able to explore the entire file system of the computer and, using command line network utilities, move to other computers on the ship's network.

Other Cyberthreats to Shipboard Computer Systems

Direct physical attacks on computers and networks remain a viable insider threat to the cybersecurity of a ship. Some researchers have reported finding "mystery systems" present on shipboard networks. These are systems that few crew members even know are present, much less what they are for or when they were installed. Invariably, these systems are ignored, unpatched, and undocumented.

Another threat is the ubiquitous USB thumb drive or memory stick. Any number of formal studies and informal experiments have demonstrated that if a person finds a stray USB memory device, they are highly likely to plug it into a computer. In most cases, a thumb drive found lying around has legitimately been lost by someone and contains standard, mundane files. In many cases, however, the thumb drive is left by a cyberattacker and contains exploit software that will execute as soon as it is plugged into the right kind of computer, usually—but not always—a Microsoft Windows system.

Creating a nefarious thumb drive does not require a super-hacker. A product called the *USB Rubber Ducky* can be purchased inexpensively on the Internet and is a keystroke injection tool disguised as a thumb drive. When plugged in, the thumb drive is seen by a Windows system as a keyboard; the computer then accepts pre-programmed keystroke payloads loaded on the thumb drive, which can be crafted by the attacker using a simple scripting language or downloaded from the Internet. This device can be used to drop any sort of program onto the infected computer, including providing the attacker with remote access. Once on the system, the attacker may be able to move throughout the network. Indeed, if the proper contents are placed on the thumb drive—music, pornographic images, or other “interesting” files—the thumb drive might be passed around by crew members and will infect many systems, possibly on more than one vessel, further increasing the cyberattacker’s likelihood of success.

Regulatory Guidance for Vessel Cybersecurity

Organizations such as the American Bureau of Shipping (ABS), the Baltic and International Maritime Council (BIMCO), and the International Association of Classification Societies (IACS), have produced cyberdefense guidance documents related to ships; these will be discussed in Chapter 8. One regulatory mandate—IMO 2021—is worth discussing here.

In June 2017, IMO released Annex 10 to Resolution MSC.428(98), which provides guidelines on maritime cyber risk management in Safety Management Systems (SMS). IMO encourages maritime administrations to ensure adherence to these guidelines no later than the first annual verification of a company’s Document of Compliance after January 1, 2021—hence the reference to this requirement as *IMO 2021*.

IMO 2021 is a cyberdefense framework for ship owners and operators comprising hardware, software, and crew training. It describes three primary pathways to reduce the cyberattack surface. First, complete a regular cyber security audit to assess cyber management, and to identify and define roles and responsibilities related to cyber risk management. Second, ensure that all software is kept patched and up-to-date. Finally, enhance employees’ cyberawareness with training, particularly related to attacks directed at people (e.g., phishing attacks and scam e-mails). IMO 2021 also requires regular, routine review of the cyber risk management plan.

Conclusion and Summary

This chapter has examined some of the many attack vectors on a ship. The use of ICT has grown so fast in the maritime industry over the last half century, and particularly in the last two decades, that it is difficult to keep up with them, even for cybersecurity professionals trained in deterrence. The systems interconnect and interact in very complex ways, making it hard to defend against every possible attack vector. Yet, just because it is difficult does not mean that it is not necessary or doable. New security weaknesses are reported constantly, and it is the responsibility of maritime manufacturers to fix the vulnerabilities and for maritime consumers to insist that fixes be produced and the patches actually applied. If we don’t take these actions, then we are responsible for our own failures.

This chapter mentioned GNSS, AIS, and OT but, very noticeably, only in passing. These topics are discussed in more detail in the next two chapters.

Chapter 6: Navigation Systems

Introduction

Shipboard navigation systems have evolved tremendously since humans started traveling on the open ocean. Mariners relied on their experience, intuition, and knowledge of nature and the seas for more than two thousand years before the introduction of instruments in the second century. The evolution from the astrolabe and charts to maritime chronometers and radio-assisted navigation took another 500-700 years. In the last 100 years, we have seen radio, radar, and satellites assist in accurate position, navigation, and timing (PNT) systems.

This chapter focuses on cybersecurity vulnerabilities of the most widely used navigation system on boats, namely global navigation satellite systems, particularly GPS, and the Automatic Identification System for situational awareness.

Integrated Navigation Systems

The command center of a vessel is the bridge, the place where the monitoring and management of all of the ship's control systems are coordinated. An integrated navigation system (INS) comprises the hardware and software on the bridge where all functions related to navigation and safe operation are consolidated into a single console or suite of displays. An INS integrates the input from many of the ship's subsystems, including:

- AIS
- Autopilot
- Echo sounder
- Electronic Chart Display and Information System (ECDIS)
- GPS/GNSS
- Navigational telex (NAVTEX)
- Gyroscope
- Navigation workstation
- Radar
- Sonar
- Sensors (e.g., rate-of-turn, rudder position, salinity, water temperature, and weather)

These inputs provide a ship's master with awareness about the state of the ship and its surrounding environment. All of the devices are interconnected via standard interfaces, such as serial lines, the Controller Area Network (CAN) bus, or Ethernet, and communicate using standard protocols. Most of the devices employ the Windows operating system or a manufacturer's proprietary operating system.

An INS is susceptible to a number of cyberattack vectors by someone who exploits the standards-based communications lines or protocols. In one demonstration, researchers used a USB thumb drive that contained a nefarious script and plugged it into one of the devices connected to the INS. The malware infected the ECDIS and was able to manipulate the apparent GPS signals by spoofing the GPS messages in the communications protocol used between the INS-attached devices. This attack could also crash the operator station, effectively blinding the ship.

Global Navigation Satellite Systems Overview

GNSS is the generic term for the four satellite navigation systems with global coverage, namely China's BeiDou, the European Union's Galileo, Russia's Global'naya Navigazionnaya Sputnikovaya Sistema (GLONASS), and the U.S.'s Global Positioning System. There are also two regional systems, the Indian Regional Navigation Satellite System (IRNSS), also known by its operational name Navigation with Indian Constellation (NavIC), and Japan's Quasi-Zenith Satellite System (QZSS). Each operates independently of the others.

Every navigation system has its own constellation comprising 18-30 medium Earth orbit (MEO) satellites, operating over several orbital planes at an altitude of 12,000-15,000 miles (19,000-23,000 km). A GNSS receiver determines its location on the Earth's surface—latitude, longitude, and altitude—using a process called *trilateration*, where the device measures its distance from the known position of three satellites.

Because the satellites travel at a speed of 2.4 miles per second (4 km per sec.), the trilateration error can be as much as one mile (1.6 km). The receiver needs to communicate with a fourth satellite to correct the clock drift and obtain the precise timing from which to determine a precise position fix; a one nanosecond (one-billionth of a second) timing discrepancy can result in a one-foot (30 cm) position error. GNSS positioning can be accurate to within about 3 ft. (1 m).

The importance of GNSS to deliver precise timing for critical infrastructures cannot be over-stated. All telecommunications networks, whether carrying voice, audio, video, or data, and operating at hundreds to trillions of bits per second, are digital in nature. These systems cannot function unless the sender and receiver know when a bit time slot begins, and this cannot happen without very precise timing. Additionally, the power grid, some Network Time Protocol (NTP) servers on the Internet, financial networks, transportation systems, and other critical infrastructure elements rely on the precision timing provided by GNSS.

The Global Positioning System

NAVSTAR, the Global Positioning System, was initiated in the late 1960s by the U.S. Air Force and U.S. Navy; the first satellite was launched in 1978 and civilian GPS equipment became available in the 1990s. Currently managed by the U.S. Space Force, GPS provides PNT services to both military and civilian users around the world. The GPS constellation employs 31 satellites, each of which orbits the Earth approximately twice a day.

In its original incarnation, GPS offered an encrypted Precise Positioning Service (PPS) for U.S. and allied military, and an unencrypted Standard Positioning Service (SPS) for civilians. SPS provided slightly less positioning precision than PPS by the introduction of controlled timing errors. By presidential order, the geolocation precision of GPS has been the same for both military and civilian applications since 2000.

GPS Jamming

Jamming refers to deliberate interference with a GPS signal, generally accomplished by distorting or overpowering the original signal so that the receiver cannot obtain its positional fix. Although the signal is transmitted at 50 watts (W) of power, the signal arrives at the surface at a fraction of a watt.

Although illegal to use, GPS jammers can be purchased at low cost over the Internet. In one early case, a truck driver in New Jersey employed a GPS jammer to hide where he was during his breaks. He inadvertently jammed Newark Liberty Airport's GPS system during trials of its automatic aircraft landing systems.

GPS jamming, which is a low-cost GPS hacking mechanism, can have serious results. Consider the many locations around the world where pilots rely on GPS to bring increasingly larger vessels through narrow shipping channels such as the Bab el-Mandeb Strait, Bosphorus Strait, Panama Canal, Strait of Gibraltar, Strait of Hormuz, Strait of Malacca, or Suez Canal.

It is possible for GPS receivers to detect signal jamming attempts, and several GPS products include that capability. These products can, in many cases, ignore (based upon its direction) or use AI to filter out, the jamming signal and recover the original GPS signal. Possibly the best mitigation against jamming is to use GNSS receivers that employ multiple constellations, such as GPS and GLONASS; using more than one satellite navigation system not only provides redundancy in case one system fails, but also the ability to cross-check the accuracy of both.

GPS Spoofing

Spoofing refers to the deliberate transmission of bogus positioning signals so that a GPS receiver miscalculates its position. Because military GPS receivers employ encrypted signals, they are less susceptible to spoofing than civilian devices unless the military encryption keys are somehow compromised.

Spoofing generally involves a third-party using specialized equipment to generate false GPS navigation signals in order to mislead a receiving device. *Meaconing* (or *masking beaconing*) is a form of spoofing where a third-party intercepts and rebroadcasts legitimate navigation signals on the proper frequency but at a higher power than the original signals to which the receiver was listening. In either case, the receivers obtain a false navigation position.

Incidents of spoofed GPS signals have grown so rapidly in the last few years that the technique has become a strategic weapon of conflict and a major threat to commercial shipping. The first highly publicized civilian GPS spoofing incident occurred in the Mediterranean Sea in 2013. This activity was coordinated by researchers from The University of Texas at Austin (UT), who caused the 213 ft. (65 m) yacht WHITE ROSE OF DRACHS to alter her course and heading, unbeknownst to the crew. The team used commercial, off-the-shelf products to build the spoofing device. The event started with the broadcast of very low-power GPS signals; the signal power was slowly increased until the ship's receiver accepted the new signal and dropped the legitimate one. The UT team's signals made it appear that WHITE ROSE had drifted three degrees to the left, a shift so slight that the crew assumed it was due to wind and current; the crew compensated for this drift by shifting the vessel slightly to the right, which eventually took them about 3,300 ft. (1 km) off course. (Additional examples of GPS spoofing, coupled with AIS spoofing, are described below.)

A variety of methods can be used to detect GPS/GNSS spoofing, and some are built in to some GNSS products. One method is to monitor for the signal distortion that occurs at the instant when the bogus signal overpowers the

legitimate signal.

A second method detects the fact that the bogus signal is coming from a different direction than the legitimate signals; in fact, whereas legitimate GNSS signals require communication with four satellites, a bogus signal generally comes from a single source. A third method is for the GPS unit to correlate the encrypted signal to ensure that it is authentic; even though the civilian unit cannot read the encrypted signal, it can ensure that it is present. Another protection, of course, is to use a receiver that can monitor multiple GNSS constellations.

The U.S. Department of Homeland Security has developed a Positioning, Navigation, and Timing (PNT) Program with a mission to protect against GNSS/GPS spoofing. Their program includes the PNT Integrity Library, a scalable framework for GNSS-based PNT manipulation detection intended for use by GNSS receiver manufacturers and GNSS-based timing server services to verify the integrity of received GNSS data and ranging signals, and the Epsilon Algorithm Suite, a set of anti-spoofing algorithms to enable end-users with basic spoofing detection capabilities. In May 2021, the Institute of Electrical and Electronics Engineers (IEEE) approved the P1952 working group to develop standards for resilient PNT user equipment.

Satellite-based PNT augmentation systems, largely using low Earth orbit (LEO) satellites, are under development to supplement GPS. LEO satellites, in particular, can provide greater precision and higher-power signals, and such systems are currently under development.

Automatic Identification System

The Automatic Identification System is a VHF radio-based scheme that operates across a 10-20 nautical mile (nm) radius and provides the capability for vessels at sea to be aware of each other's presence. AIS messages broadcast over the air are described in International Telecommunication Union, Radiocommunication Sector (ITU-R) recommendations and are based on NMEA 0183. (This section does not address AIS messages sent between devices within the skin of a ship.)

The purpose of AIS is to give maritime authorities the ability to identify and monitor vessels and cargo in its area of responsibility, and for ships and shore stations to exchange navigation, meteorological, safety, and other vessel-related information. The impetus for such a situational awareness system was the 1989 grounding of EXXON VALDEZ in Prince William Sound, Alaska, and the subsequent oil spill. AIS was designed in the 1990s and adopted internationally in the 2002 International Convention for the Safety of Life at Sea (SOLAS).

The SOLAS accord is broad in scope and covers a range of critical themes associated with maritime situational awareness. Chapter V ("Safety of Navigation") of the SOLAS agreement specifies the types of ships required to carry *Class A* AIS transceivers, and includes ships of 300 or more gross tons traveling internationally, commercial power vessels longer than 64 ft. (19.5 meters), and power vessels certified to carry more than 150 passengers. Military vessels are specifically exempted from the requirement to transmit AIS information, although most modern warships have both public and encrypted AIS capability.

Class B AIS transceivers are used on large yachts, small fishing and other commercial boats, ocean-going personal vessels, and other vessels that carry AIS equipment but have no legal requirement to do so. Class A devices generally transmit more detailed information with more power than do Class B devices, including the ship's name, International Maritime Organization (IMO) registration number, Mobile Maritime Service Identity (MMSI), dimensions, latitude and longitude, course, heading, rate-of-turn, destination, type of cargo, and operational status. AIS requirements in the U.S. are specified in the United States Code of Federal Regulations (CFR).

AIS today is an essential part of a ship's integrated navigation system, used primarily for situational awareness and collision avoidance among vessels. AIS devices obtain location information from the ship's GNSS, and are therefore highly dependent on the integrity of the positioning system. AIS is also now widely used by ports, vessel traffic management services, and coastal surveillance agencies.

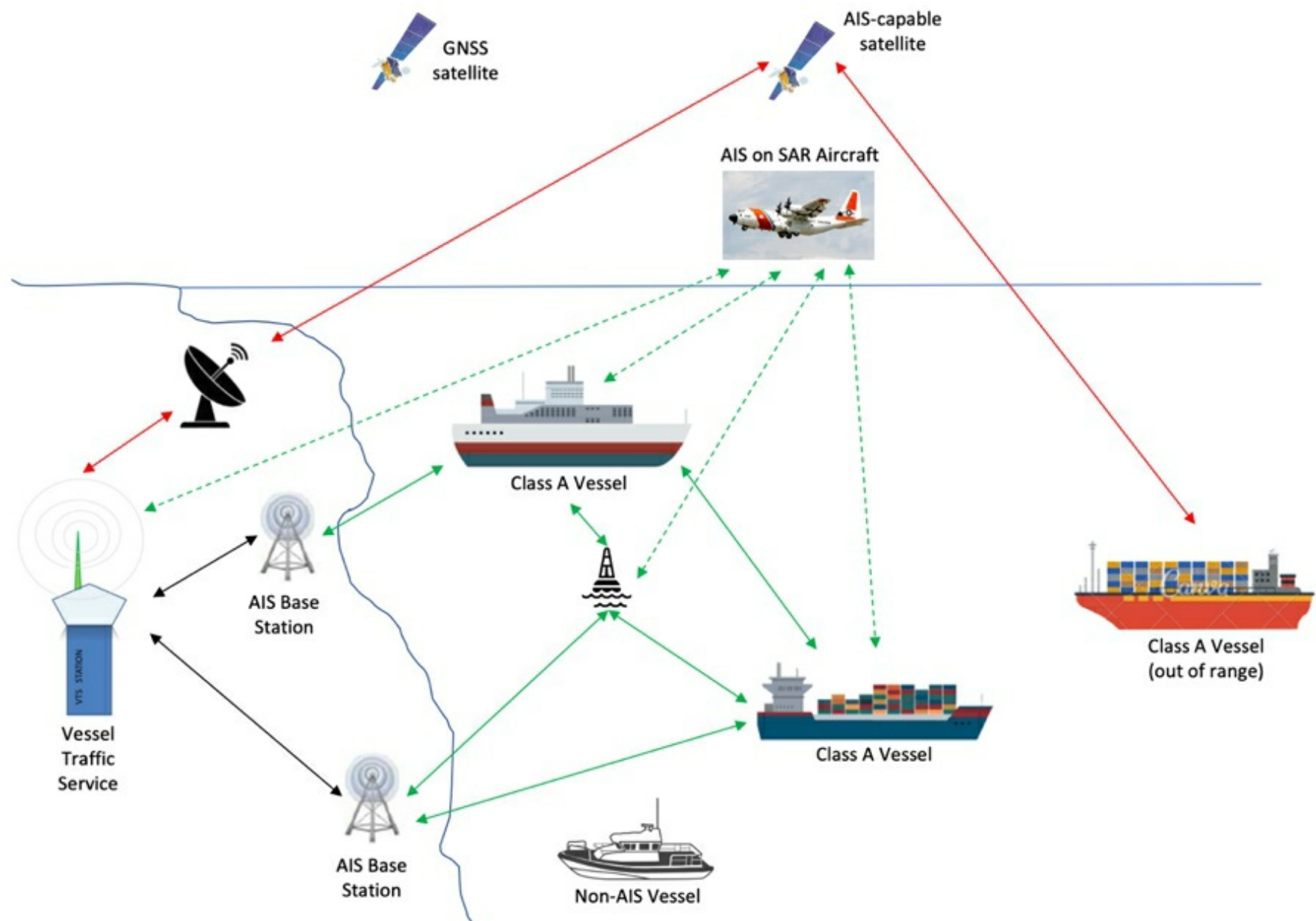


Figure 6.1. Stations in the AIS network.

Figure 6.1 shows the active components in the AIS network, including ships and boats, AIS-equipped satellites, search and rescue (SAR) aircraft, AIS base stations, repeaters, and specially equipped aids-to-navigation. Other AIS-capable mobile stations include SAR transponders (AIS-SART), man overboard (MOB) transmitters, and Emergency Position Indicating Radio Beacons (EPIRB). GNSS satellites are not a direct component of AIS, but they provide geographic positioning information essential to the operation of AIS.

AIS Security Vulnerabilities

AIS was designed in the 1990s without much thought about protection from active attacks. There are a number of known vulnerabilities with the AIS protocols:

- *Lack of geographic validation:* It is possible for a device to transmit an AIS message from one location while purporting to be in another.
- *Lack of timestamp information:* AIS transmissions do not include a date and time. A Bad Actor can record valid AIS messages and retransmit those messages later, making it appear that a vessel was present at another time.
- *Lack of message authentication:* Without a mechanism to authenticate the sender of a message, anyone with the ability to transmit an AIS packet can impersonate any other AIS device.
- *Lack of message integrity:* There is no mechanism to ensure that AIS messages are sending correct and valid information. A fishing boat could, for example, pose as a different type of vessel.

These vulnerabilities would allow anyone to intentionally craft bogus messages to spoof a ghost (i.e., non-existent) vessel or aid to navigation (ATONs), replay earlier AIS traffic to confuse legitimate vessels' situational awareness, trigger false SAR or closest point-of-approach (CPA) alerts, or send bogus weather or navigation information. Each of these scenarios could possibly cause another vessel to alter its course. Because all AIS transceivers transmit over public VHF frequencies, anyone can eavesdrop on the radio traffic and, in fact, an individual could jam the AIS signals, effectively causing a DoS attack that causes a small area of the AIS network to go dark. These attacks are enabled by software tools that can generate and interpret AIS messages, and are commonly available on the Internet.

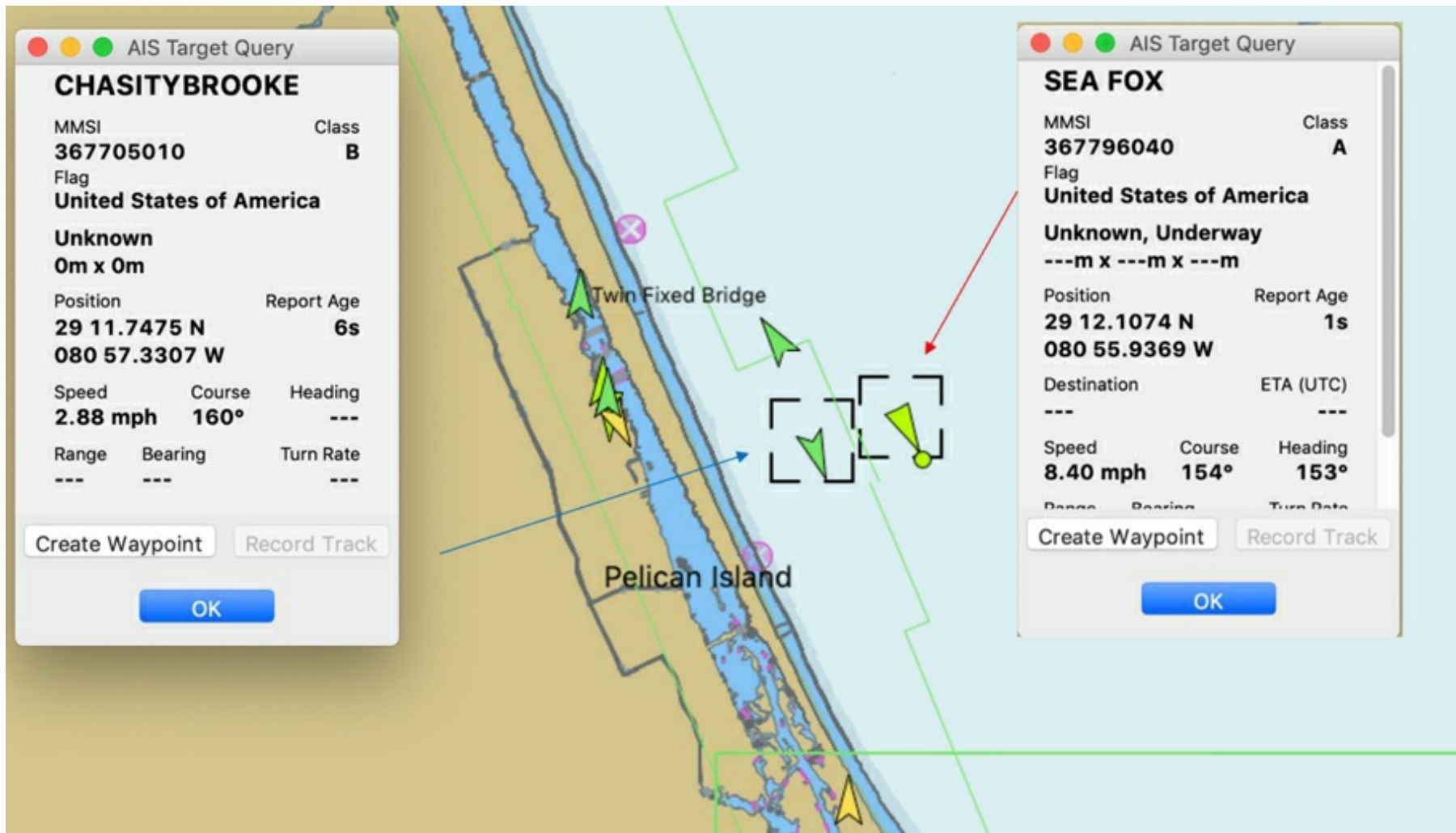


Figure 6.2. AIS display of real (CHASITYBROOKE) and ghost (SEA FOX) vessels off the coast of Daytona Beach, Florida.

Figure 6.2 is a display showing an AIS replay attack, and the appearance of ghost vessels on an AIS display. This image shows symbols for nine vessels in the area of Daytona Beach, Florida, including the details for two of the boats. CHASITYBROOKE and six of the other targets are real vessels, actually present at the time that this image was taken. SEA FOX and one other target are also real vessels but had actually been in the area six months earlier; their position reports are being replayed and interjected into the AIS data stream. It is impossible to tell from AIS alone which ships are real and which are “ghosts.”

Figure 6.3 shows how ghost ATONs can be used to create a fake channel. The display shows the red and green buoys in Ponce de Leon Inlet on the east coast of Florida, marking the portion of the inlet that is deep enough for safe passage. Also shown is a set of virtual ATONs that include a preferred channel marker (labelled “PI”) and virtual red/green ATONs defining a second channel on the shallow south side of the inlet. These virtual ATONs appear based upon spoofed AIS messages. The U.S. Coast Guard has sole authority in the U.S. to transmit information about virtual ATONs, but there is no AIS mechanism with which to authenticate the sender of this information.



Figure 6.3. AIS display of real ATONs and fake virtual ATONs in Ponce De Leon Inlet, Florida.

A variety of secure or encrypted AIS solutions have been implemented to create, in essence, private AIS subnets. Several mechanisms to add security to the open, public AIS network have been proposed but are not likely to be implemented in the foreseeable future due to the cost and requirement to maintain backward compatibility and device interoperability.

Case Studies: GPS and AIS Spoofing

The University of Texas' theoretical demonstration of GPS spoofing in 2013 was shown to be practical in June 2017, when a GPS spoofing event involving nearly 20 vessels occurred in the Black Sea. In this incident, the master of ATRIA, a 37,500-ton tanker off the Russian port of Novorossiysk, reported that his GPS showed his ship to be 20 nm (37 km) away at Gelendzhik Airport (Figure 6.4). Navigation systems from at least 20 nearby ships showed them all to be at the same location. As a consequence, closest point of approach alarms on many vessels indicated imminent collisions.

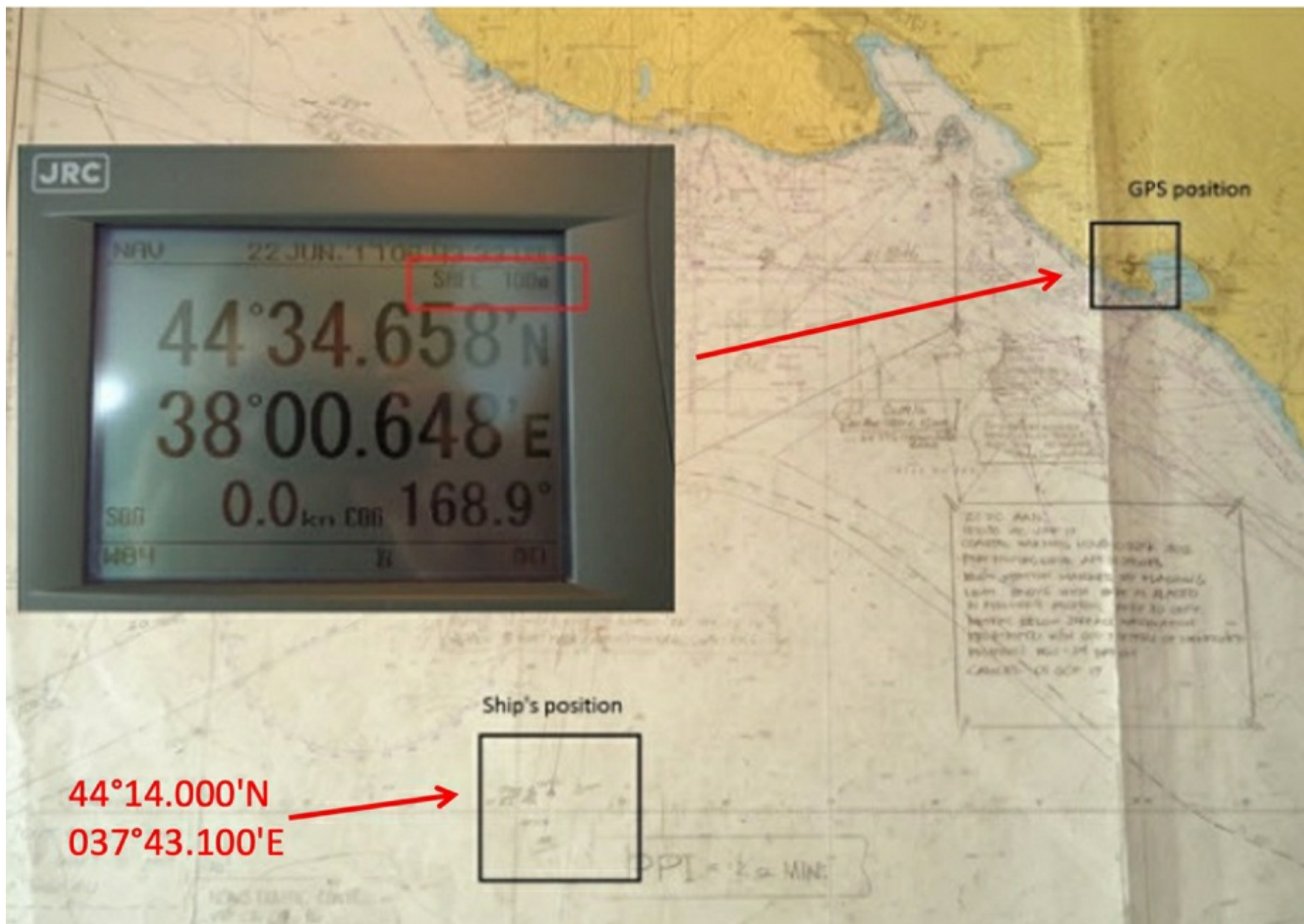


Figure 6.4. GPS display on board ATRIA during a spoofing event, showing reported versus actual position.

It was widely speculated at the time that the Black Sea spoofing event was due to Russian electronic warfare. Subsequent reports have shown that this incident was part of a larger pattern of GNSS interference in Russian waters, placing ships at multiple airports, including Sochi, St. Petersburg, and Vladivostok.

Reports of GNSS signal interference, signal loss, and reduced position accuracy in the Eastern Mediterranean Sea were first reported as far back as 2018 and continue to this day, affecting areas from Cyprus and the coast of Egypt to Israel and Saudi Arabia. The IMO, USCG, U.S. Maritime Administration (MARAD), and other maritime groups have issued multiple advisories about these episodes, which appear to continue unabated. Some researchers have noted that GNSS outages are a common occurrence all over the world around commercial shipping lanes.

GNSS spoofing is believed to have played a role in the seizure of STENA IMPERO in the Strait of Hormuz in July 2019. The U.K.-flagged oil tanker was seized when Iran claimed that the ship was in the wrong channel when exiting the Strait, thus violating international law. A satellite track of the vessel shows that STENA IMPERO was proceeding normally through the Strait before making a sudden turn toward Iranian territorial waters. It is also widely believed that Iran seized the tanker as retaliation for the impounding of an Iranian-controlled oil tanker by the U.K. in Gibraltar a few weeks earlier due to Iran's violations of European Union (EU) sanctions.

GPS and AIS spoofing have evolved in seriousness, complexity, and impact since 2017. The first of a new trend was a July 2019 incident in the Port of Shanghai. According to reports, the 700 ft. (213 m) container ship MANUKAI was in the Huangpu River headed toward her assigned berth. The ship's master reported that AIS displayed another vessel moving at 7 knots (kn) in the same channel. The other ship then suddenly disappeared and, after a short period of time, re-appeared at the dock. This pattern later repeated, with the other ship showing up on the display, moving in the channel at 5 kn and then 2 kn, disappearing entirely, and then reappearing back at the dock. The master of MANUKAI was able to visually locate the other vessel and confirm that it had never left its dock. As MANUKAI reached its own assigned berth, its GPS receivers and all navigation systems suddenly failed, and the captain was unable to get an accurate fix.

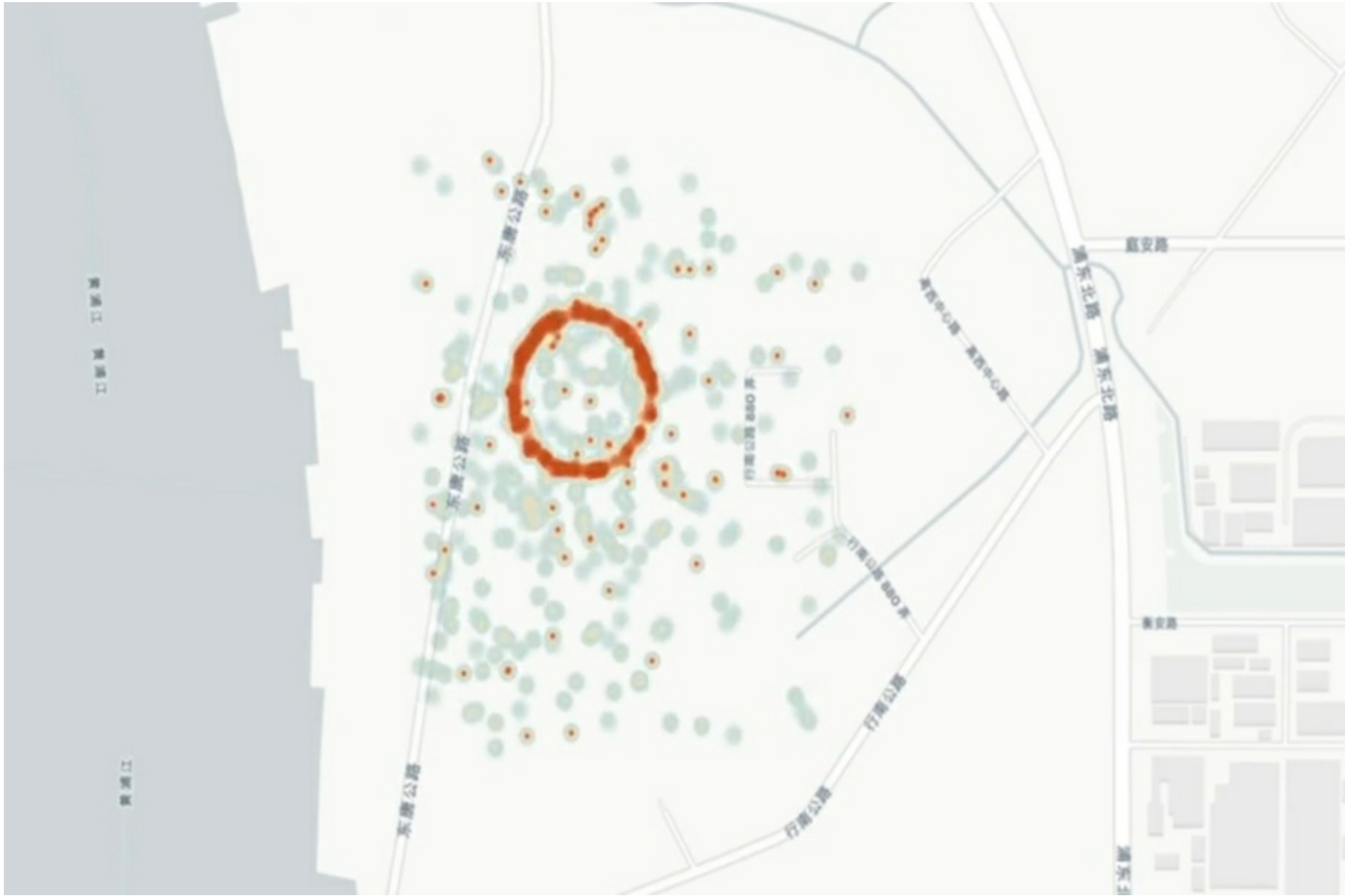


Figure 6.5. GPS circle spoofing in the area of the Huangpu River near the Port of Shanghai.

Additional analysis of AIS data showed that similar GPS spoofing incidents had occurred in the Shanghai area for at least a year prior to the MANUKAI incident. In that year, the intensity and quantity of GPS spoofing events increased, hitting a peak of nearly 300 on the day of the MANUKAI event. But that's not what makes this spoofing incident most significant. Previously-reported Russian spoofing placed all of the affected vessels together at a single point. In Shanghai, the spoofed ships appeared to jump around every few minutes to locations that seemed to concentrate in large circles, primarily on the east bank of the Huangpu River (Figure 6.5). An analysis of the data shows almost daily spoofing attacks affecting vessels of the Huangpu Maritime Safety Administration (MSA); one MSA boat was spoofed 394 times in a nine-month period.

AIS spoofing is also a part of the Port of Shanghai story. Smugglers in the area often spoof AIS signals from other, legitimate vessels to escape detection by the authorities. The Shanghai MSA reports that vessels carrying banned sand and gravel accounted for 23 collisions or allisions^[20] on the Yangtze River in 2018, with the loss of 53 lives. In June 2019, a tanker suspected of smuggling oil had been sending cloned AIS signals; it reportedly rammed an MSA patrol boat to evade capture.

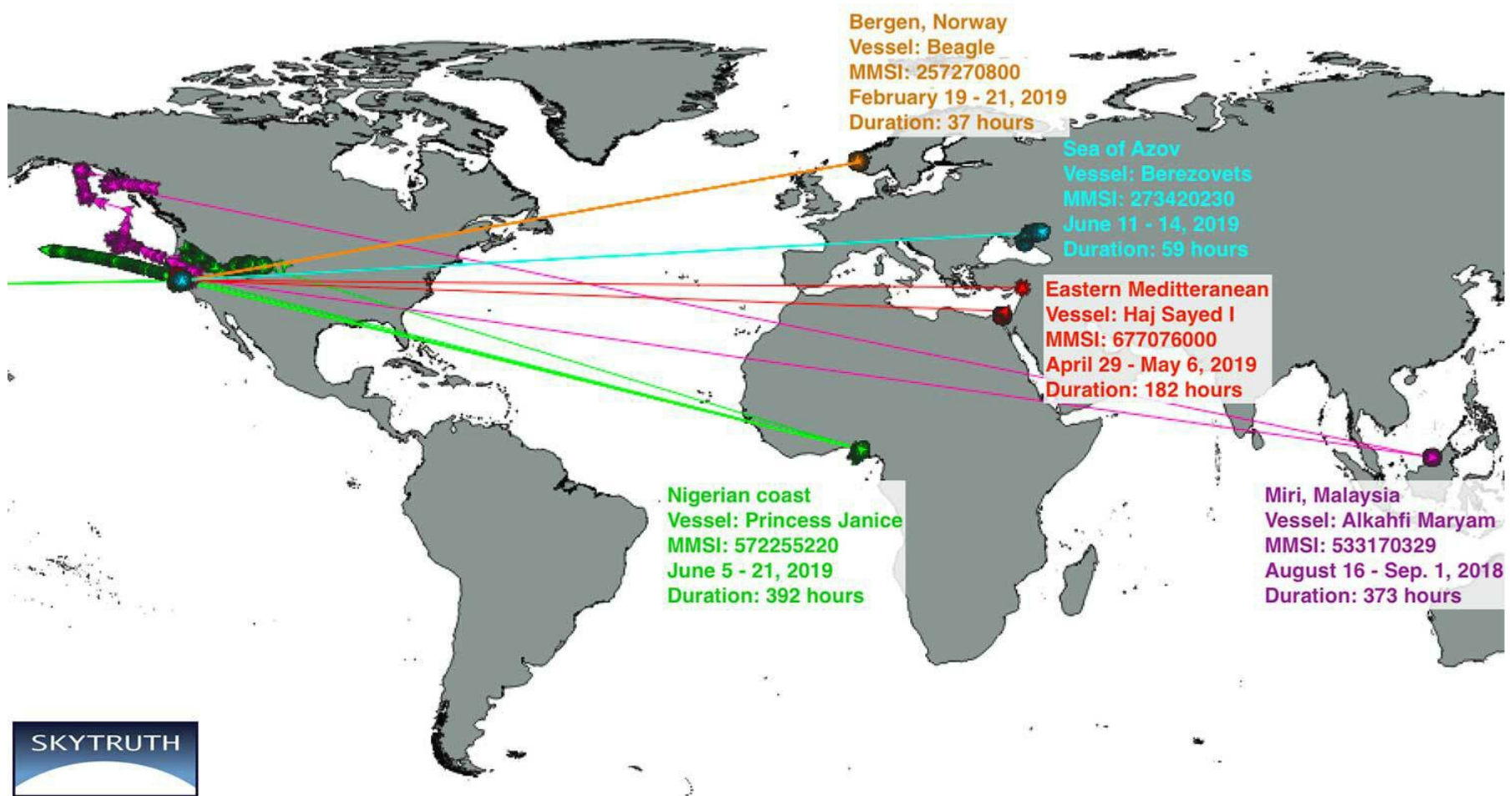


Figure 6.6. Actual location of vessels seeing *circle spoofing* off Pt. Reyes.

These GPS and AIS spoofing issues are by no means limited to China and Russia, and they certainly show no signs of diminishing. So-called *circle spoofing* of GPS has been reported in Iran and other locations around the world. In an alarming escalation of attacks on GPS and AIS, several vessels in 2018 and 2019 reported that their AIS data showed them to be traveling in circles in the area of Point Reyes, just north of San Francisco (Figure 6.6), although their true positions were confirmed to be in different locations in the Eastern Hemisphere, thousands of miles away.

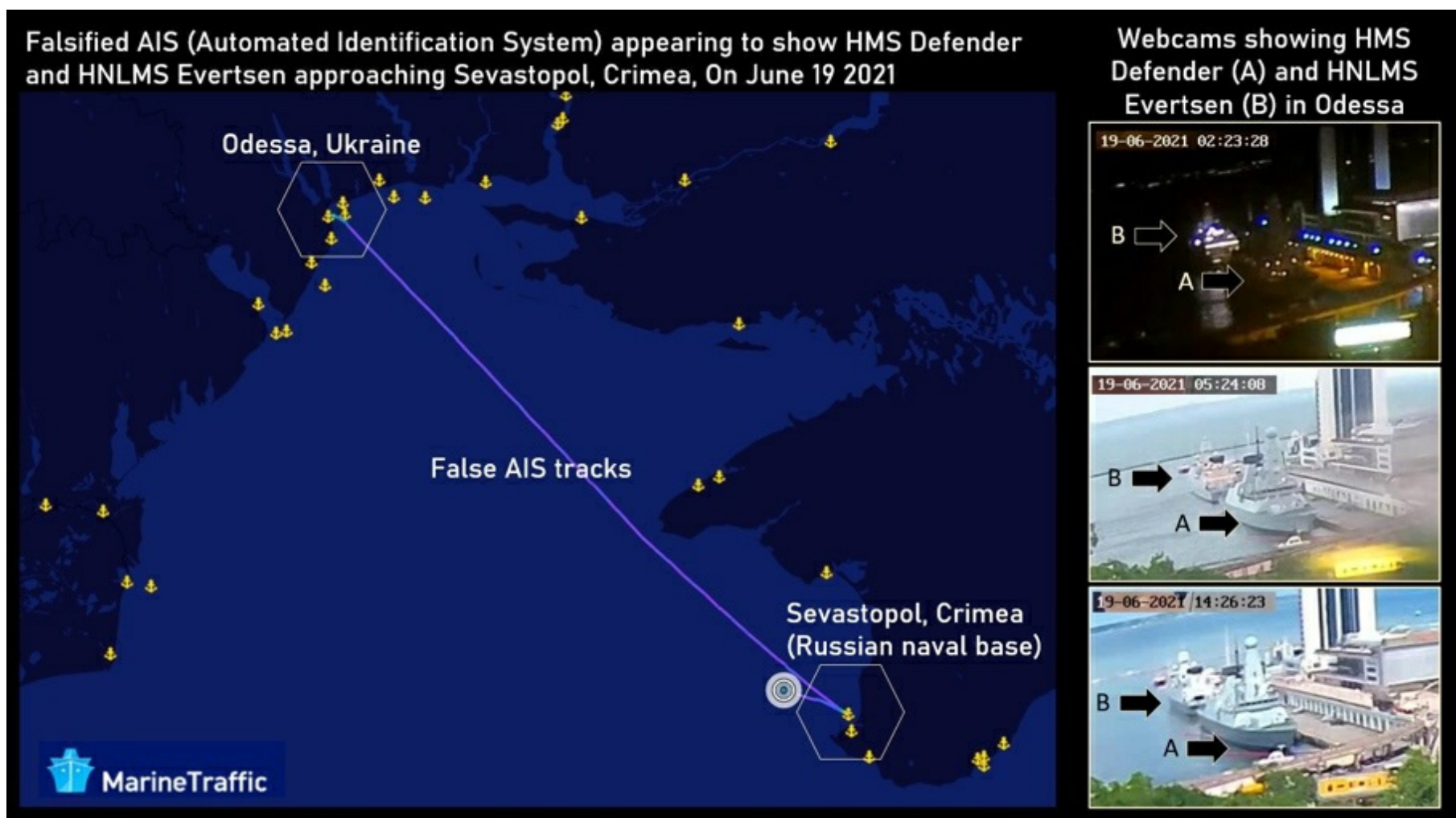


Figure 6.7. AIS spoofing in the Black Sea.

Incidents of GPS and AIS spoofing continue to escalate, and the potential consequences become more dangerous as time goes on. In mid-June 2021, two NATO warships—the U.K.’s HMS DEFENDER and Dutch HNLMS EVERSTEN—arrived at the Ukrainian port of Odessa. AIS tracking information showed both vessels leaving Odessa late that evening on a direct path to Sevastopol, Crimea, passing within two nautical miles of the port housing Russia’s Black Sea fleet headquarters (Figure 6.7). Despite what the AIS tracks showed, however, live webcam videos, real-time images from third-party weather sites, and eyewitnesses confirmed that both vessels were in Odessa that night and the next day.

Russia annexed Crimea in 2014, an action widely criticized by the international community. Most nations do not recognize Crimea as Russian territory, and this remains a point of contention between Russia and NATO. Indeed, days after the AIS spoofing event, Russian policymakers complained that their maritime patrols were forced to fire warning shots at DEFENDER to keep her out of Russian territorial waters. The U.K. denies that such an event ever took place; instead, they claim that DEFENDER was making a routine passage in a recognized traffic separation pattern in Ukrainian waters while Russia was conducting pre-announced gunnery practice miles away. Russia also claims that a patrol plane dropped bombs in her path while the U.K. denies that any such event occurred. And all of this took place in the weeks prior to NATO's annual exercises in the Black Sea, slated to commence in late-June 2021. Later in June, similar AIS tracks showed the USS ROSS near the Crimea, even as Web cam footage and other evidence suggests that the ship never left its dock in Odessa.

More than 100 incidents of false AIS warship tracks have been reported since mid-2020. These spoofs have affected more than a dozen European nations, as well as Russia and the U.S. One of the largest such incidents occurred in September 2020, when bogus AIS tracks of HMS QUEEN ELIZABETH and five escort vessels en route towards the Irish Sea were generated. Satellite imagery showed an empty ocean at the purported time of the AIS tracks, and, in fact, the six vessels were not even together at the time.

Students of history can draw parallels to the Gulf of Tonkin incidents that led to the escalation of U.S. military activity in Vietnam in the 1960s. The first incident occurred in early August 1964 when USS MADDOX was attacked by three North Vietnamese patrol boats; MADDOX fought back the attack with minimal damage and no casualties to herself. There was no subsequent U.S. plan to respond or retaliate. The second incident occurred two days later when MADDOX and another U.S. warship, USS TURNER JOY, reported being under attack based upon radar images. TURNER JOY fired at targets showing on radar and aircraft were deployed from the USS TICONDEROGA, although the pilots could not visually confirm seeing attacking vessels. In fact, this second attack never occurred. Documents declassified several decades later reveal that the ships' radar was only mimicking attack boats. The misinterpretation of the signals intelligence supported the narrative that the North Vietnamese were systematically and deliberately attacking U.S. Navy vessels in international waters. Even without confirmation of a second attack, the U.S. Congress passed the Gulf of Tonkin Resolution, providing the authorization for the U.S. to start offensive military action in Vietnam.

Use of AIS spoofing is not limited to nation-states or offensive actions. In August 2020, a large Chinese fishing fleet operating off the coast of the Galapagos Islands was accused of falsifying its GPS location in attempts to mislead regulatory agencies while it was operating in prohibited shipping grounds. Global Fishing Watch (GFW) claimed that the fishing vessels were transmitting GPS signals indicating their position between the Chatham Islands and mainland New Zealand, 6,200 miles (10,000 km) from the Galapagos, even though no Chinese fishing vessels were near New Zealand at that time.

The problem is much larger than this single example. In June 2021, Oceana, the maritime conservation advocacy group, released analysis showing rampant fishing fleet spoofing, with hundreds of fishing boats "disappearing" from AIS off the coast of Argentina. GFW's analysis of AIS data from 800 foreign fishing vessels from 2018-2021 found 6,000 gaps in ships' transmissions that lasted at least 24 hours, totaling more than 600,000 missing hours. Hiding fishing vessel locations is most likely done to mask potential illegal, unreported, and unregulated (IUU) fishing activities, or otherwise skirt regulatory boundaries. Chinese vessels accounted for 66% of the incidents.

AIS spoofing can also mask other clandestine activity using *vessel identity laundering*, where a "dirty" (e.g., criminal) ship takes on the AIS identity of a "clean" ship to evade detection, sanctions, inspection, etc. Usually, the intent is to defraud IMO, other vessels, regulators, or maritime authorities. In 2018, for example, M/V YUK TUNG falsely spoofed M/V HIKA, which was 3,780 nm (7,000 km) away, during a suspicious ship-to-ship transfer at sea. In 2019, M/V FU XING 12 manipulated its identity and location by employing two AIS onboard transponders and four different ship names to disguise illegal coal operations in China and North Korea. In 2021, vessels involved in a North Korean fuel smuggling operation were found to be using fake AIS identities.

Conclusion and Summary

GNSS, particularly GPS, and AIS, are key elements for safety at sea, not to mention all of the non-maritime applications of PNT systems. The technology behind GNSS and AIS is impressive, yet the systems are surprisingly susceptible to inexpensive, low technology attacks by adversaries that range from criminal syndicates to nation-states. GPS spoofing, in particular, has become increasingly more sophisticated in the last few years. Initially, GPS spoofing caused a single vessel to veer a bit off course. In the next iteration, multiple vessels all believed themselves to be at the same point some tens of miles away from their true location.

Next, vessels in a particular geographic area were made to believe that they were in multiple locations—in a circle pattern—a few miles away. In later ploys, vessels saw themselves at multiple locations in a circle pattern thousands

of miles away from their actual position. Finally, warships are being spoofed in addition to commercial and merchant vessels. No loss of life has yet been directly attributed to GPS and AIS spoofing, but that is a logical outcome of the ever-escalating war on PNT technologies. Countering AIS and GPS jamming and spoofing will be a particular concern for the maritime industry, standards organizations, and governments in years to come.

The next chapter discusses cybersecurity issues related to industrial control systems, operational technology, and other forms of automation in the maritime industry.

Chapter 7: Operational Technology and Autonomous Systems

Introduction

The genesis of the modern general-purpose computer began in the 1940s. Businesses started to routinely use huge, expensive mainframe computers in the 1950s. Because of the development of the transistor, we saw the arrival of microprocessors by the end of the 1960s, and personal-class computers by the end of the 1970s. Moore's Law, which observes that chip density doubles and the price halves every two years, kicked in by this time, so that today we all have a telephone in our pocket that is really a quad-core, portable Internet terminal.

Computer networks also evolved during this era. Packet switching, the underlying technology of almost all wide-area networking today, was invented in the 1960s. In 1969, the ARPANET, the beginning of today's Internet, became operational. By that time, telephone companies were already starting to imagine the integrated digital network (IDN), a single network on which all types of data could flow, and all types of devices could be interconnected.

So, why this walk down memory lane? Today's mobile phone is so much more than a telephony device. It also manages high-speed data connections to the Internet and other networks. It contains the ability to connect to a telecommunication carrier's data network, a local Wi-Fi or Bluetooth network, or GPS. It contains sensors to measure temperature, humidity, movement, and balance. Fundamentally, we have developed—and now carry in our pockets—a device with which we can call another person, send e-mail or text messages, take a picture, engage in a two-way video session, send or receive money, obtain positional awareness, or manage our home's smart refrigerator.

We have realized the dream of the IDN, albeit with another name. Today we call it the Internet of Things, a scheme that allows computers to control and manage hardware. From your phone, you can check the security camera at your house. From the bridge of your ship, you can also manage the tension on the lines making you fast. The maritime industry has embraced the IoT concept for a number of reasons, forming what some call the "Shipboard IoT" or "Internet of Ships." Maritime applications of IoT allow better management and control of shipboard systems and the very vessel itself, onloading and offloading of cargo, and various levels of autonomous devices.

A *thing* in the Internet of Things is often a sensor with the ability to respond to a specific change in its environment by spewing a small bit of data to some sort of controller. Ship listing too far to port? Spew data. Water level in a remote stock tank on a ranch too low? Spew data. Patient blood pressure dipping below a defined threshold? Spew data. Mooring line slack? Spew data.

The data generated by IoT sensors is transported over a digital network to a central location, often *the cloud*, where it can be aggregated and analyzed. The cloud is one or more data centers that offer on-demand storage and computing. The analyzed data yields insights, which can be acted upon by a human or machine-based process to take corrective action.

This chapter reviews some of the underlying technology enabling the IoT, describes applications, defines terms and concepts, and addresses some of the cybersecurity vulnerabilities that come with IoT on our ships and at our ports.

Cyber-Physical Systems, Operational Technology, and the Internet of Things

Cyber-physical systems (CPS) is an umbrella term that gathers people, computers, and physical devices into an operational, functional system. CPS takes advantage of the development of more sophisticated sensors, instruments, network protocols, and embedded computers, and combines them to build smart infrastructures and industrial applications. Some common CPS applications include the smart grid; medical monitoring; autonomous vehicles, vessels, and aircraft; process control systems; robotics systems; and automatic aviation and maritime navigation systems.

CPS and IoT are part of the computer and telecommunications evolution resulting from *digitization* and *digitalization*. Both of these terms refer to evolutions in technology that are transforming the MTS—and other critical infrastructures—in momentous ways.

While deceptively similar, these terms address two different important concepts. *Digitization* refers to the conversion of an analog process into a digital one, without necessarily altering the process itself. By way of example, voice, music, and video have analog content and used to be carried or stored on analog communications

media (i.e., sine waves). Today, these forms of communication are carried as a series of zeroes and ones on digital communications facilities (i.e., square waves).

Digitalization is a transformational leap, providing the ability to integrate all forms of information over a single network backbone and, therefore, provide an infrastructure supporting applications and hardware that can manage and synthesize all of that data at once. To continue the example above, we have today a single network that can integrate voice, radio stations, television stations, streaming video, interactive multi-player games, and Internet services (including data transfers) on a single network out to a single device over a single cable (or other telecommunications channel). In the late-1990s and early-2000s, this coming-together was sometimes called *convergence*.

Digitization also provided the ability for the collection, storage, analysis, and study of historical data. Digitalization allowed for the aggregation of data from multiple inputs, providing huge data sets from which we can better understand our systems. This has led us to an era of big data, machine learning (ML), and artificial intelligence (AI). The acceleration of change in the digital world continues at a rapid pace and will impact all aspects of the maritime industry, from shipping lines and ports to regulations and information security. This is the intersection of the MTS and Industry 4.0.^[21]

Operational Technology

Operational technology comprises the many technologies and methods that enable the cyber and physical worlds to come together (Figure 7.1). In OT systems, computers directly provide real-time monitoring and control of physical devices such as valves, pumps, switches, dams, assembly lines, power grids, robots, and transportation systems.

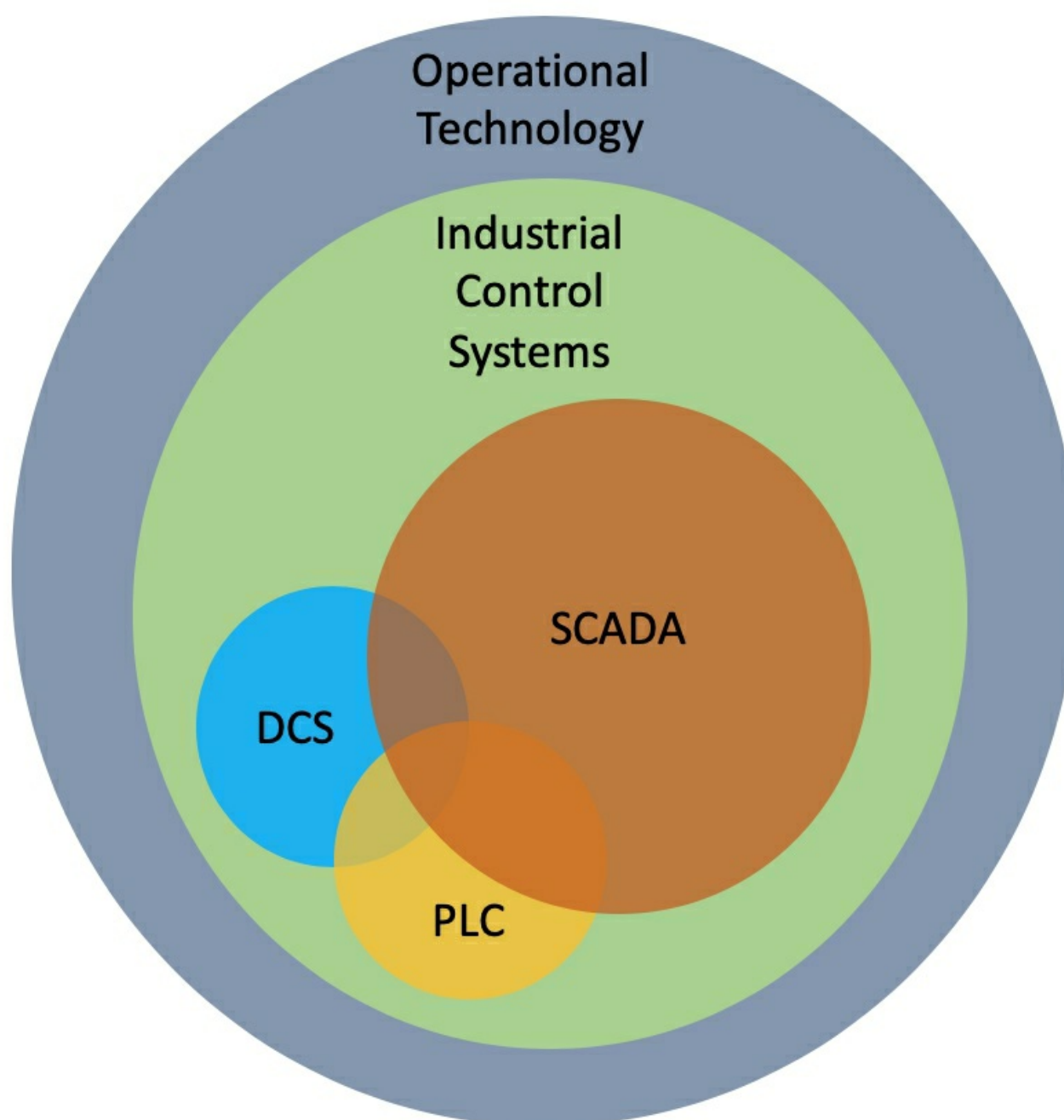


Figure 7.1. A classification of OT devices.

Industrial control systems (ICS) make up the largest segment of OT devices. ICS generally refers to computing systems that manage industrial operations and other CPS applications, and controls equipment in the physical world. ICS differs from information and communications technology systems, which generally manage administrative operations and data.

The performance, reliability, and security requirements of ICS software and hardware are different from those of traditional ICT (Table 7.1). The biggest overall difference is that ICS manages 24/7/365 operational environments where the controls require real-time management, low-delay communication, and high-availability hardware and

software. The results of ICS breakdown due to device failure or cyberattack can be disastrous, not just to the device itself but to the surrounding operational environment and safety of nearby individuals.

Information and Communication Technology	Operational Technology
Performance	
Non-real-time	Real-time
Response must be reliable	Response is time critical
High throughput demanded	Modest throughput acceptable
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 the field acceptable	Thorough QA/QC testing expected
Modifications possible with little paperwork	Formal certification of changes might be required
Security Priorities	
Risk impact: Loss of CIA and business operations	Risk impact: Environmental and safety, as well as business operations
Recover by rebooting	Fault-tolerance/redundancy essential

Table 7.1. Operational requirements of ICT versus ICS.

ICSs include a variety of control subsystems. A programmable logic controller (PLC) is a special-purpose computer that controls hardware devices in an industrial automation environment. The PLC receives data from sensors and other input devices, processes the data, and sends control commands to the managed hardware. As an example, the Stuxnet attack (discussed earlier in this book) was directed at the PLCs controlling specific models of Siemens centrifuges, which is why Stuxnet had no impact on Windows systems that did not have the PLC or on the Windows operating system itself.

A distributed control system (DCS) manages processes that usually have many feedback loops and are distributed among many controllers, but without a central management system. A DCS, for example, might comprise many PLCs networked together, each operating independently of the others but all reporting back to a central operator's control station. In this instance, it is the DCS that provides the logic of the distributed system to make it appear as one, while the PLCs implement the control function. An example might be a ship's propulsion system, where monitoring and management of the engines, drive shafts, and propellers can occur at a central console, which is made aware of the status of the individual components by a variety of sensors.

Finally, Supervisory Control and Data Acquisition (SCADA) systems provide a high level, central management environment whereby operators can maintain situational awareness about, and manage, a distributed ICS. SCADA systems integrate network communications, a graphical user interface, and multiple data acquisition capabilities so that a human operator can monitor the state of a system, detect abnormal activity or system status in near real-time, and adjust the processes as necessary.

The Internet of Things

The Holy Grail of cyber-physical systems is the Internet of Things. The realization of a concept from the late 1960s, IoT combines myriad enabling technologies in new ways to offer new services and applications. In many ways, IoT combines ideas that have been around for decades—but for which there was no supporting technology—with new methods and ideas. IoT combines data analytics, artificial intelligence, widely available broadband networks, advanced sensor technology, miniaturized processors, and new software to allow individual, independent devices to share information and engage in network-wide decision making, transforming traditional physical devices into smart systems. These enabling technologies are not necessarily new; the innovation is in how these ICS and ICT building blocks are assembled to support an endless array of machine-to-machine (M2M) and people-to-machine (P2M) applications.

No one should believe for an instant that IoT and its derivatives are just another fad or pie-in-the-sky idea; IoT is quite real. There were 15.4 billion IoT devices worldwide in 2015, doubling to 30.7 billion by the end of 2020, and with an estimated 250% jump to 75.4 billion by 2025, meaning an average of nine IoT devices per person. IoT applications are found throughout critical infrastructures, businesses, and recreation, including smart cities, healthcare, agriculture, supply chains, power supplies, retail and distribution, and transportation. Within the transportation sector, we already see smart cars, airports, and rail; within the MTS, we have smart ships, smart ports—and smart seas.

The dramatically higher speeds and reduced latency associated with Fifth Generation (5G) broadband cellular networks coupled with IoT technologies will create new convergence and digitalization opportunities. It is hard to overstate the significance of these new applications and services to the maritime domain.

IoT Cybersecurity Issues

IoT systems are composed of physical devices and the computers that monitor and/or control them. Computers within CPS and IoT networks are prone to vulnerabilities for the same reasons that any other computer has vulnerabilities, namely, the system architecture, the operating system, the network that interconnects the components, the application software, and user policies and procedures. Cyberthreats can come from hackers, user error, failures of hardware or software, or external failures outside the control of the system.

One thing that makes CPS special is that a cyberattack on an OT computer can actually damage hardware. One of the first such demonstrations of this threat vector was the 2007 DHS Aurora Generator Test. In this case, a cyberattack disabled the generator's built-in safety mechanisms, allowing the machine to vibrate sufficiently that it broke itself up within just a few minutes.

As discussed in an earlier chapter, Stuxnet was most likely the first malware in the wild known to attack hardware, in this case PLCs for centrifuges controlled by Siemens Step7 software. While Stuxnet was the first, it is not the only example of malware to attack hardware; CrashOverride and Trisis/Triton, for example, are families of malware that specifically target ICSs associated with power grids and utility systems.

OT-based control systems can respond to abnormal events more quickly and efficiently than a person. But these systems must be fully understood by the human operator and there must be a way for the operator to override the automatic controls. The automatic trim system in the Boeing 737 MAX 8 provides an object lesson for the maritime industry. Because the flight stability characteristics of the 737 MAX are different and more difficult for pilots to manage than earlier 737 models, Boeing installed an automatic trim system called the Maneuvering Characteristics Automation System (MCAS) to aid the pilots and better control the aircraft. In two crashes of the 737 MAX in 2018 and 2019, however, the system overcorrected and pilots could not override MCAS to regain control of the airplane; in the case of the 2019 crash of Ethiopian Airlines Flight 302, the pilots and MCAS exchanged control several times during its six-minute flight.

Unsecured IoT devices are a very real threat to the global Internet and other devices attached to the Internet. IoT devices are a favorite target for cybercriminals because of the enormous attack surface presented by so many devices with network access, and the fact that the billions of devices represent enormous computing power if harnessed together as a botnet. Such a botnet could be used as a platform for even larger cyberattacks, such as the DDoS attacks described in an earlier chapter. IoT devices often rely on the perimeter security of the network to which they are attached for protection. As a result, many such devices have poor built-in security, such as insecure Web-, mobile-, or cloud-accessible interfaces; inadequate tools with which to configure security parameters; weak authentication and authorization mechanisms; and a lack of encryption. The IoT network itself has several points of weakness, as well, including the sensors, hardware controllers, communications network, and the back-end IT systems, plus other potential vulnerabilities specific to the application or the hardware. And while there are ways to reduce the vulnerability of an IoT-dependent environment—through edge device network segmentation, for example—the practice is not always incorporated because of cost, complexity, lack of awareness, hubris, or other factors.

The Internet of Things—and the associated OT—is real and is providing significant cost savings and efficiencies in many aspects of life. But the bottom line here is that there are still risks that must be mitigated. The FBI released a public warning about potential exploitation of IoT devices as far back as 2017. As noted earlier, there are websites such as *censys.io* and *shodan.io* that allow someone to search the Internet for IoT devices, and other sites where one can find passwords to hacked IoT devices (many of which have fixed, unchangeable passwords). There is no question that ICS devices are a target of the hacker community and a huge number of IoT devices are vulnerable to cyberattacks.

The lesson is... use of IoT is growing. Embrace the new technology and the innovation that it can bring to the MTS, but treat security seriously and think about it when designing any OT installations.

Defining Cyberattacks in a Cyber-Physical World

Given the tight linkage between software, network communications, and physical devices in operational technology and IoT systems, the nature of a cyberattack requires a re-examination.

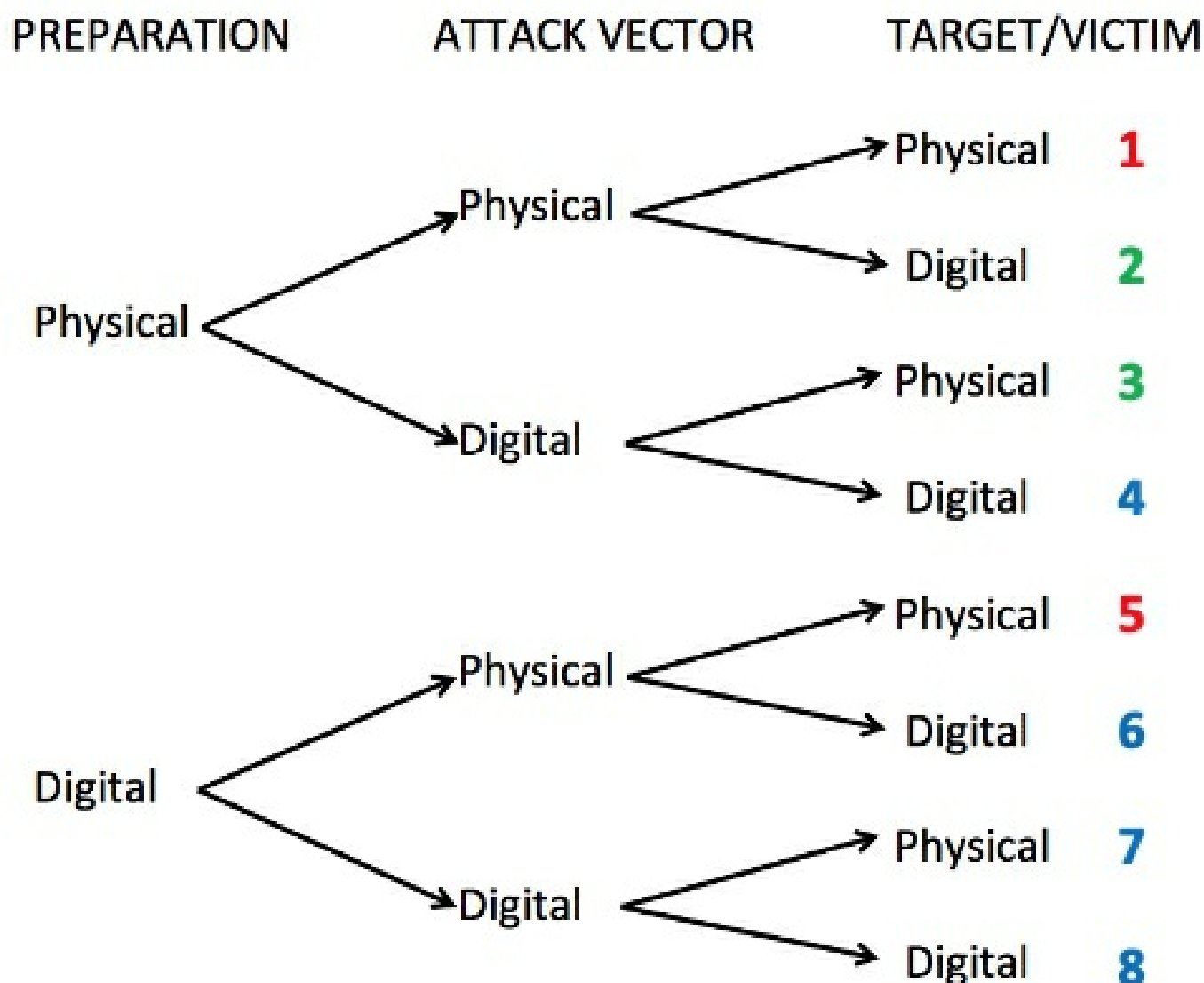


Figure 7.2. Attack pathways in a cyber-physical world.

Think of any cyberattack as having three phases: preparation, the actual attack, and the ultimate target compromise. Each of these phases can have a physical or digital vector (Figure 7.2):

- An attacker can prepare their attack by performing online reconnaissance (e.g., Google maps or public websites) or a physical presence (e.g., staking out a port or obtaining insider information).
- The attack can be carried out using cyber tools (e.g., malware) or physical weapons (e.g., a bomb).
- The target can be a digital device (e.g., a server) or a piece of machinery (e.g., a crane).

There are eight possible combinations of physical/digital attack pathways in the preparation-attack-target attack chain. Any attack where at least two of the factors are *digital* can most likely be classified as a cyberattack (paths 4 and 6-8), whereas an incident where the attack vector and target are both *physical* would probably not be (paths 1 and 5). The remaining two options, where exactly two of the factors are physical (paths 2-3), are not clearly one or the other. The real lesson here, however, is not a rule about what is or is not a cyberattack in this environment but, instead, recognizing which of the preparation-attack-target paths above can form a viable intrusion on an OT system. This is an important awareness exercise because an intended attack could conceivably be thwarted at any one of the three stages.

Maritime OT Applications and Cybersecurity

From an ICT perspective, cargo and passenger ships have become increasingly complex over the last half-century. As computers became smaller and more mobile, shipboard automation could be introduced to assist and inform crew and engineers with hull, mechanical, and electrical (HM&E) systems, shipboard electricity, propulsion and maneuvering systems, ballast systems, and cargo systems. As a result, ship operations have largely become safer, more efficient, and more manageable with fewer crew members. In many cases, automation provides a level of precision that a human cannot achieve or maintain, such as the exact steering of a course or holding a precise position. As more automated systems are introduced onto a vessel, those systems become increasingly inter-dependent.

As suggested above, IoT devices can be employed for any number of functions in the MTS, limited more by our creativity than by technology. Researchers are beginning to coin terms such as Shipboard Internet of Things (SIoT)

and Internet of Ships (IoS) to denote current and new ICT systems combined with IoT technologies, new types of sensors, and OT that can allow system designers to build any number of integrated shipboard control systems, from the bridge to the engine room.

The endgame of applying IoT technologies pervasively to ships yields the concept of *smart ships*. Smart ship systems can offer:

- Advanced collision avoidance capabilities.
- Optimization of trip planning, routing, and fuel utilization.
- Monitoring and management of all vessel systems, such as propulsion, ballast, and power generation, as well as hull stress.
- Monitoring the local environment, including water temperature and salinity.
- Supplements to the traditional Interactive Electronic Technical Manual (IETM) maintenance systems, automatically collecting and analyzing system data in order to optimize the detection and repair of faulty equipment before a catastrophic failure occurs.
- Optimized supply chain operations, ensuring that fuel, food, and other supplies are available to the ship as needed.

As a master comes to know more about the state of their vessel, the entire operation becomes more efficient, provides more effective financial management, and yields a safer shipboard environment. This information can also be used to optimize supply chain operations, ensuring that fuel, food, and other supplies are available for the ship when needed.

These new OT and IoT technologies have also enabled new and innovative systems outside of the ship as well, such as:

- Intelligent mooring systems that embed sensors in mooring lines. The lines can monitor tension, time, and temperature, and provide early detection of wear and failure. The crew can monitor the line status from the bridge via an app.
- A Cooperative Cognitive Maritime Cyber Physical System (CCMCPS) can provide high-speed and low-cost communication between ships, ports, buoys, offshore platforms, and shore stations. At ports, these systems can offer full or partially automated cranes and transport vehicles. Cargo vessels are consistently getting larger and container vessels have become a fast-growing segment in the shipping industry. Ports, then, have become the bottleneck in the movement of cargo. To help overcome this challenge, a CCMCPS can optimize communication between vessels, ports, maritime terminals, and cargo handling systems.
- The U.S. DoD Advanced Research Projects Agency (DARPA) Ocean of Things (OoT) project aims to achieve persistent maritime situational awareness by deploying thousands of low-cost, intelligent floats that drift as a distributed sensor network. Each float is designed to collect data about the local environment (e.g., temperature, salinity, sea state, and location) and activity (e.g., commercial vessel traffic, aircraft, and marine mammal migration).

Maritime OT implementations have the same potential security issues as any computer or IoT system. 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 related hardware and smartphone apps to monitor and control ship engines. In 2018, this ICS suite was found to have several system backdoors, as well as authentication and encryption vulnerabilities, including use of an undocumented remote access server with a hard-coded username and password, an undocumented inter-device communication protocol without any validation procedures, cleartext transmission of sensitive information, and an embedded Web server that transmits the administrator's personal identification number (PIN) in plaintext. If exploited, an attacker could access and control any connected engines, determine what sensors are active on the ship's network, determine the system configurations and settings, and send arbitrary control messages to the engine control units. These specific examples are similar to flaws found in many types of OT devices. The lesson is that these systems need to be built from the ground up with security in mind.

Although cyberdefense strategies often focus on external cyberattacks, there are other factors leading to device failure and information becoming unavailable, such as system congestion and traffic load, radio interference with wireless devices, roaming issues with mobile IoT devices, and interoperability issues with other devices. Information security is not only about perimeter defense from outside Bad Actors; it also requires excellent network and system design.

Smart Ports

As discussed in an earlier chapter, as the nexus of maritime operations, ports comprise a complex infrastructure of ICT, machinery, business processes and transactions between trading and supply chain partners, regulations, and stakeholders that include port owners, port authorities, port operators, unions, shipping and other transportation companies, public safety agencies, and, in some cases, the military.

IoT technologies, OT, big data, and AI provide a way for ports to improve their operational efficiency. By using a combination of sensors, gauges, cameras, radio-frequency identification (RFID), and other IoT devices coupled with advanced technologies such as GNSS, Internet, Wi-Fi, and 4G/5G mobile communications, the efficiency of port operations can be significantly improved. Better organization and timing of ship movements in a busy port can optimize transit, berthing, and cargo loading/ unloading, which can save both ports and shipping companies tens of thousands of dollars for every hour of decreased down time. For that matter, container terminals can be automated to optimize the interoperation of cargo ships, rail-mounted gantry cranes, and automatic guided vehicles, in addition to optimized intermodal transfers of cargo.

A pioneer in the use of smart port technology is the Port of Rotterdam, the largest seaport in Europe. The port, with an area of 41 square miles (106 sq. km), is 25 miles (40 km) long, and handles 125,000 ships and 8.5 million cargo containers annually. The Port employs IoT technology to gather information that provides situational awareness to the port authority, data for traffic management services, and information about the vessels themselves. Sensors measure water temperature, depth, current speed and direction, tidal flows, wind direction and speed, berth availability, and other parameters that feed centralized information to a control center that is also available on a dashboard app on connected vessels. In conjunction with specialized AIS messages, this flow of information can reduce vessel wait times; optimize dock, load, and unload times; and maximize the throughput of vessels at cargo terminals. Similar smart ship management, intelligent traffic flow, and smart port logistics systems are being implemented at other ports around the world.

Smart ports are enormous implementations of hardware, software, and communications, including the development of new apps. The potential for attacks on OT hardware and software is always present. A Bad Actor could, for example, hack or otherwise manipulate a sensor sub-system to send incorrect data to the central control system, or bogus smart port app messages could be sent to the dashboard. In addition, vessel traffic could be sorely disrupted should an attacker send false AIS Clearance Time to Enter Port, Berthing Data, or Tidal Window messages. Any of these scenarios could disrupt port operations, potentially for days at a time.

IoT and OT are the enablers for many advanced applications within the port of the future. Digital ropes, mentioned earlier, will allow the master of a vessel to better monitor mooring line status, tension, and wear. Virtual reality will enhance new crew training and scenario planning opportunities. Virtual Reality will provide enhanced analysis of maritime operations and real-time scenario response. Emerging sensor technologies will measure any number of vessel, port, and cargo environmental parameters. Drones will take on an increased role in ports for inspection and monitoring of vessels, cargo, and vehicles, as well as widen the perimeter for visual situational awareness. Three-dimensional (3D) printing at ports, or even on vessels, will allow faster repairs in some instances—but is also subject to hackers either crashing the printer or altering the printer’s design files in order to impact the output. Digital twins will provide a way to inexpensively simulate new ways of deploying technology. The capability of the technology is truly limited only by our imagination. However, as more and more IoT devices are deployed, and because of the relative security weaknesses of those devices, OT and CPS will remain an attractive target for cybercriminals and other cyberattackers.

Autonomous Operations in the MTS

The natural evolution of smart devices, artificial intelligence, machine learning, big data, and IoT is autonomy in maritime shipboard and shore-based operations. This section describes how the convergence of thousands of years of maritime technology and a half-century of computing and communications technology offers a new future for the MTS.

Level	Ship Autonomy
0	No autonomy
1	Minimal crew required
2	Partial automation; local crew for simple tasks
3	Conditional autonomy, potential intervention by local crew
4	High autonomy, mostly self-running
5	Complete autonomy

Table 7.2. SAE-based levels of ship autonomy.

The term *autonomous* as applied to shipping means different things to different people. A common classification is to use a modified version of the Society of Automotive Engineers (SAE) taxonomy for autonomous automobiles (Table 7.2). As the table suggests, autonomy can range from a vessel with a remote captain at the controls to a

remote-controlled vessel with a standby crew on board to a fully autonomous ship.

Autonomous Commercial Vessels

The commercial maritime industry is actively pursuing research in the area of autonomous ships for a variety of practical reasons. The first is safety. The majority of maritime accidents are caused by human error, and many of those are due to fatigue. Autonomous vessels, with or without a remote operator, can remain alert 24/7.

Additionally, automated systems can respond more quickly and efficiently to unexpected events.

A second reason is the increased cargo capacity of a vessel without a crew. An autonomous cargo carrier can be designed to optimize space for cargo containers; there is no need for structures such as decks, a bridge, crew quarters, and galley, nor for crew-oriented environmental and safety systems.

Third, autonomous vessels promise a more efficient operation. Ships can be designed to be more wind resistant and streamlined, resulting in lighter, more efficient, less expensive to operate, and more fuel-efficient vessels.

An additional compelling reason for use of autonomous vessels is to address the difficulty in finding trained merchant mariners for the growing commercial fleets. Ships have become increasingly dependent on computers, OT, and other automation, thus merchant mariners need both traditional maritime and modern technical skills to operate today's vessels. At the same time, it is harder to attract young people from developed nations to seek careers in the merchant marine service, particularly given the long times at sea away from friends and family, as well as dangers such as weather and piracy.^[22] To this latter point, some industry observers have suggested that a crewless vessel might be less likely to be targeted by pirates because there are no hostages to take.

Research into, and trials of, autonomy in commercial maritime shipping have been ongoing since 2012, mostly in Asia and Europe. One of the earliest demonstrations was in December 2018, when Finferries' car ferry FALCO operated in a fully autonomous mode on a one-mile (1664 m) outbound trip and under remote control on the return trip. A captain monitored the vessel from an autonomous operations center 30 miles (50 km) away. FALCO demonstrated Rolls-Royce's Safer Vessel with Autonomous Navigation (SVAN) technology.

In February 2020, Bastø Fosen, Kongsberg, and the Norwegian Maritime Authority commenced a trial with semi-autonomous passenger and vehicle ferry BASTØ FOSEN VI. The 469 foot (142.9 m) ferry operates under fully automated control from dock to dock, with a captain and full crew on board for oversight, on a seven-mile (11 km), 30-minute route.

In April 2020, Royal Caribbean conducted an unplanned remote trial of a shipboard autonomous system. Due to COVID-19 travel restrictions, Dutch shipbuilder De Hoop could not bring subcontractors to ships for sea trials. In preparation for a late-2020 maiden voyage of Silversea Cruises' SILVER ORIGIN, a remote trial of its dynamic positioning system, intended to keep the ship within four inches (10 cm) of a fixed point, was conducted. During the trial, a subcontractor tuned and calibrated the system via a fast Internet connection from 1,120 miles (1,800 km) away in St. Petersburg, Russia. The ship's captain was on board and acted as lookout.

The Mayflower Autonomous Ship (MAS) project is a global consortium, led by IBM and Promare, intended as the first trial of a full-sized, open ocean, autonomous vessel (Figure 7.3). The 50 foot (15 m) fully autonomous vessel MAYFLOWER will rely on solar, diesel, and wind power, and will employ artificial intelligence, deep learning, and standard maritime technologies to manage the crossing. Originally scheduled to start the 3,220 mile (5,182 km) trip from Plymouth, England to Plymouth, Massachusetts in September 2020 on the 400th anniversary of the voyage of sailing vessel MAYFLOWER, the trip was postponed due to COVID-19. In June 2021, MAYFLOWER started its voyage but had to turn around due to a minor mechanical failure, as there was no one on board to affect a repair. The vessel was re-launched in September 2021 and the next attempt for the Atlantic crossing is scheduled for 2022.



Figure 7.3. Mayflower autonomous ship.

In May 2021, the Norwegian University of Science and Technology (NTNU) launched a full-scale prototype of an autonomous, all-electric urban passenger ferry (Autoferry). The Autoferry is intended to provide an on-demand passenger ferry service across urban rivers and other small waterways; a passenger could get on the ferry, press a button, and automatically be taken to the other side, not unlike an elevator taking passengers up and down in a building. The Autoferry also employs electrical propulsion with automatic battery charging, high-precision GNSS navigation plus backup, and an anti-collision system.

Japan has a number of autonomous shipping research programs under the administration of the Nippon Foundation. The MEGURI 2040 project, announced in early 2020, focuses on the development of fully autonomous vessel navigation systems and is supporting five project consortia. The Designing the Future of Full Autonomous Ship (DFFAS) Project, announced in mid-2020, is composed of 30 industry and research companies. The DFFAS Fleet Operation Centre (FOC) near Tokyo was completed in September 2021. The underlying goals of DFFAS are to build a sustainable society and advance maritime technology, with a target of half of Japan's domestic coastal vessels operating autonomously by 2040.

In September 2019, NYK Line conducted the first trial of an autonomous cargo vessel, IRIS LEADER, off the coast of Japan under an onboard crew's supervision. NYK Line has started a conversion of its entire 800-ship fleet to utilize autonomous technology.

In August 2021, Nippon Yusen Kabushiki Kaisha (NYK Line) announced plans for testing the first autonomous cargo ship to traverse waters with heavy maritime traffic. The container ship will pilot itself, aided by Orca AI technology, from Tokyo Bay to Ise Bay, a 236 mile (380 km) trip planned for early 2022. Trip data—from weather and sea state to radar and traffic information—will be collected and analyzed at an onshore support center. Instructions can be sent to the ship and, if necessary, operators at the data center can remotely steer the vessel.

In January 2022, three significant demonstrations took place, operated by MEGURI 2040 consortium teams:

- A small tourism boat operated fully autonomously on a 1 mile (1.7 km) route. The unmanned vessel operated autonomously from departure to docking in the area of Sarushima Island.
- SOLEIL, a 728 ft. (222 m) automobile ferry, operated fully autonomously on a 149 mile (240 km) route from Shinmoji to Iyonada, at speeds up to 26 kn. The Shin Nihonkai Ferry Co. vessel employed a sensor image analysis system with infrared cameras, an automated ship navigation system, and an automated port berthing/unberthing system, developed by Mitsubishi Heavy Industries.
- Mitsui O.S.K. Lines (MOL) conducted the first sea trial of a fully autonomous containership, M/V MIKAGE. The 312 foot (95 m), 194 TEU vessel operated on a route from Tsuruga Port to Sakai Port using technology from Mitsui and Furuno. As above, the vessel was able to berth and unberth autonomously (with drone support for the lines), autonomous navigation, and advanced sensor technology.

An autonomous tug, NELLIE BLY, circumnavigated Denmark in October 2021. The 36 foot (11m) vessel

completed the 1,000 nm (1,852 km) voyage in 129 operational hours over 13 days, at an average speed of 7.9 kn. The boat employed the Sea Machines' SM300 sensor-to-propeller autonomy system for route planning, dynamic situational awareness, and collision avoidance. Remote captains, in Boston, Massachusetts, commanded the boat with an onboard crew of two.



Figure 7.4. Autonomous, electric containership YARA BIRKELAND.

In a project that started in 2017, YARA BIRKELAND, the world's first autonomous, electric containership, was launched in November 2021 (Figure 7.4). With a capacity of 120 TEUs, the 261 ft. (79.5 m) vessel will operate on 37 nm (68.5 km) inland/near coastal route between Herøya and Larvik in Norway. The vessel will be operated from Massterly's operations center in Horten, Norway. Operation of this autonomous, electric vessel is expected to cut 1,000 tonnes of CO₂ and replace 40,000 truckloads annually.

Regardless of the level of a ship's autonomous operation, all are dependent upon a large body of ICT, OT, and IoT technologies. Autonomous vessels will still need GNSS fixes, weather reports, radar, AIS, and other communications capabilities to maintain situational awareness and PNT functions. Additional onboard situational awareness will be provided by high-tech cameras, laser imaging, detection, and ranging (LIDAR), and equipment that will provide an overview of the area surrounding the ship. Most of the trials of autonomous vessels are taking place on inland or near coastal waters, zones that require particular diligence and offer little room for error due to the congestion of shipping and the relatively narrow channels in those areas. The technology on which the operator, ship's master, or automated piloting depends, however, is the same IoT, ICT, and ICS that we have spent the rest of this book describing in terms of their cyber vulnerability.

Autonomous vessels will also require very real operational changes, particularly when they are around other ships. As an example, international standards for training are designed for merchant mariners at sea and have not yet taken into account autonomous vessels nor crew operating from a shore station. How will a pilot take an autonomous vessel through a narrow channel or into a seaport? The maritime navigation rules of the road as described in the COLREGS are designed for manned vessels; how should an autonomous vessel meet the lookout, radar watch, and radio watch requirements?

Indeed, autonomous vessels of all sizes still need a captain, but this revolution in technology requires a re-thinking of what being a ship's master means, given that the bridge of the future might include a set of monitors, dashboard applications, and controls in the comfort of one's office or home. While the benefits and/or detriments of autonomy and remote crews are not a cybersecurity issue, per se, the implementation of this remote access surely is. It is impossible to think of safety at sea in an autonomous environment without considering the cyber risks, and it is naive to believe that remote communications with ships is immune to hacking, DoS, man-in-the-middle attacks, and most of the other cyber vulnerabilities discussed throughout this book.

The growth in autonomous shipping should take no one by surprise. Regardless of any lingering cybersecurity issues, the economic drivers and technology capability means that autonomy is here to stay. Japan alone expects the percentage of crewless autonomous coastal vessels to grow from 10% in 2030 to 50% in 2040.

Autonomous Military Vessels

Militaries around the world have the same interest in autonomous vessels as the commercial industry, but have additional imperatives, such as force multiplication, reduced cost to build a fleet of warships, the ability to field more patrol boats on the water, and the desire to keep sailors out of harm's way.

The U.S. Navy started their autonomous unmanned surface vessel (USV) in the early 2000s. One of the Navy's first

USVs was SEA HUNTER, a 132 ft. (40 m) vessel with a maximum speed of 27 kn and a range of 10,000 nm (18,520 km). SEA HUNTER has been tested operationally as part of a carrier strike force, for such tasks as mine search, detection, neutralization, and delivery; antisubmarine and surface warfare; maritime interdiction and security; electronic warfare; and support of special operations forces. A fleet of seven of these *medium unmanned surface vessels (MUSV)*—defined as between 39 ft. (12 m) and 164 ft. (50 m) in length—is expected by 2023.

The U.S. Navy's Ghost Fleet Overlord program describes a *large unmanned surface vessel (LUSV)*, defined as a USV longer than 164 ft. (50 m). LUSVs integrate command-and-control systems and payloads, and more complex naval operations. A pair of LUSVs, RANGER and NOMAD, completed the 4,400-mile (7,081-km) transit from Mobile, Alabama to Port Hueneme, California via the Panama Canal in October 2020 and July 2021, respectively. Both vessels operated in autonomous mode for 95% of the route; they were under remote manual control only while in the Panama Canal Zone.

The Chinese People's Liberation Army Navy (PLAN) launched a small surface combat vessel, JARI, in September 2018. JARI is a 50 ft. (15 m) long USV with range of 500 miles (80 km) and a top speed of 42 kn, and is designed for remote-control or autonomous operation. JARI carries the armaments of a small destroyer, including phased-array radar, sonar, a deck gun, two close-range air defense missiles, two vertical-launch silos for anti-air/anti-ship missiles, and two torpedo tubes. A next generation version of JARI with a length of 70 ft. (21 m) is already in the design phase.

In September 2019, the USCG Research and Development Center (RDC) launched DEFIANT (29RDC), a 29 ft. (9 m) autonomous response boat (Figure 7.5). Pilot testing of the vessel, which employs autonomous technology from Sea Machines, occurred in October 2020. An autonomous response boat could take on such roles as surveillance, routine patrols, SAR, and interdiction.

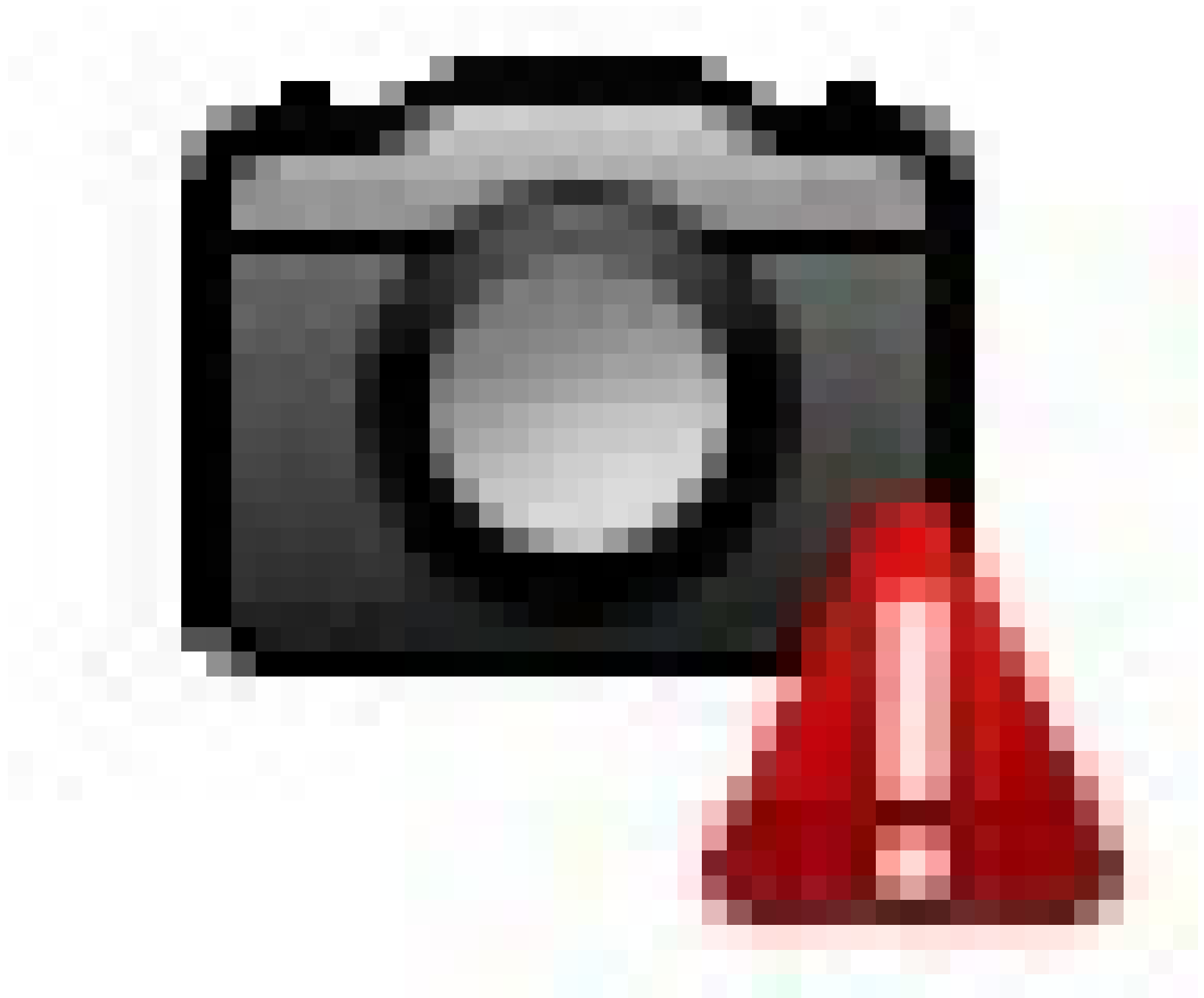


Figure 7.5. USCG DEFiant (29RDC).

Many other countries, including India, Israel, Russia, Singapore, Turkey, and the United Arab Emirates (U.A.E.) have similar USV projects underway. The cybersecurity considerations for military USVs are the same as for commercial autonomous vessels, but the implications of a successful cyberattack are significantly greater.

Other Autonomous Maritime Systems

The operation of large autonomous vessels will necessitate changes in port and other vessel-related operations. Research is currently ongoing into the use and deployment of fully autonomous and/or remote controlled harbor, terminal, and escort tugboats. One of the big challenges is the way in which the large ship and the tug interact when in close proximity to one another. Maneuvering one or more autonomous tugs around an autonomous ship is but one concern; another is how the tug couples with the larger vessel. Tests of autonomous and remote operated tugs, as well as autonomous coupling systems, have been underway since 2017 in Asia and Europe.

Another area of related research addresses in-port and offshore autonomous mooring systems. Autonomous mooring systems could be applicable with any type of large ship, but are particularly advantageous for use with autonomous ships. One system is being designed specifically for YARA BIRKELAND to provide autonomous mooring as well as autonomous cargo loading and unloading.

Autonomous maritime systems are also starting to incorporate drones, aka unmanned aerial vehicles (UAVs). Both autonomous and remote control UAVs could be used to provide aerial surveillance, thus increasing the situational awareness perimeter in a port area, for both manned and autonomous ships. Autonomous drones can supplement

ship inspectors by their ability to safely enter locations on vessels that are too dangerous for people. Outfitted with an appropriate imaging system, UAVs could provide a detailed analysis of a hull or cargo bay beyond the capabilities of a human, and do so in real-time. Autonomous UAVs might also supplement autonomous tugboats and mooring systems by performing such activities as transporting heaving lines from the dock or tug to a ship. It is likely that mariners in the future will see more UAVs in the air around ports and near coastal waters. Although well beyond the scope of this book, cybersecurity related to UAVs is an active area of research.

Conclusion and Summary

The Internet of Things, operational technology, and autonomous maritime systems are the core technologies bringing the maritime industry into the future. While the individual devices might be small, the systems are large, complex, and complete with cybersecurity issues because, fundamentally, they are merely computer hardware, software, and communications technologies. The SP800-82 Guidelines from NIST and the International Electrotechnical Commission (IEC) 62443 family of standards form a basis for ICS cybersecurity.

Up to this point, this book has addressed cybersecurity threats. We would be remiss if we painted a dark picture without providing some light. There are many organizations, agencies, and other resources that provide guidance related to cyberdefense in the MTS. That is the subject of the next chapter.

Chapter 8: Strategies for Maritime Cyberdefense

Introduction

The previous chapters of this book described many aspects of cybersecurity in the MTS, including its vulnerabilities and weaknesses, along with real case studies where those vulnerabilities have been exploited. The MTS is not monolithic; it is complex and multi-faceted. For that reason, there is no single maritime cyberdefense strategy that applies to every maritime entity. Knowledge of the myriad vulnerabilities is required to plan an appropriate cyberdefense strategy.

This chapter discusses three broad topics related to cyberdefense in the MTS: how the industry views cybersecurity and its preparedness for cyberthreats, risk management as it applies to cyberdefense, and various frameworks and organizations addressing MTS cybersecurity.

Industry Opinions

Planning cybersecurity policies and procedures requires knowing what needs to be protected and prioritizing where to put available cyberdefense assets. A 2017 IHS Markit Fairplay survey of 284 maritime executives, managers, and crew provided useful insights for cybersecurity planning, including:

- While nearly two-thirds of executives and managers said that their organization provided cyber best practices awareness training to crew and staff, less than half of crew respondents answered that question in the affirmative.
- All respondent segments indicated that people are the largest source of cybersecurity vulnerability, although executives were the least likely segment to believe so. The executives' second-highest choice was the organization's technology, while the managers' second-highest choice was their suppliers.
- 80% of crew and shore-side staff indicated that they brought their own devices into the workplace, the same percentage that stated that they log in to personal accounts while at work. Answers to later questions showed generally poor cyberhygiene practices, including users reporting opening attachments in e-mails from strangers and sharing their passwords with others.

The IHS Markit Fairplay survey in 2018 of 237 maritime managers, owners, regulators, crew, and port staff provided additional insights:

- All of the cybersecurity protection measures that respondents identified as being employed included the typical mechanisms for standard computer systems and networks, such as firewalls, intrusion detection/prevention systems, and logical segmentation of networks. The survey did not ask questions that appeared related to OT-class networks, as found on automated maritime systems.
- Respondents identified navigation systems (e.g., ECDIS and GPS) as the most vulnerable area on a vessel to cyberattack, followed by safety (e.g., VDR), propulsion, and cargo control systems.

A 2018 Jones Walker survey of 126 senior executives, chief information and technology officers, and other key players in the MTS gave a good picture of the state of maritime cybersecurity in the U.S.:

- The respondents recognize that the U.S. maritime industry is being targeted by cyberattackers; 38% of all respondents, including 80% of large companies, reported a cyberattack in the prior year, and 10% of respondents reported a successful breach.
- The MTS has a false sense of cyber preparedness. While 69% of respondents expressed confidence in the industry's cybersecurity readiness, 64% indicated that their own companies were unprepared to handle the business, financial, regulatory, and public relations consequences of a data breach.
- Large companies, as might be expected, are better positioned to handle a cyber emergency than smaller companies. All respondents from large organizations felt that their organization was prepared to prevent a data breach, while only 19% of midsize and 6% of small companies felt prepared. Respondents from 97% of large companies, 31% of midsize companies, and 8% of small companies reported having cyberinsurance.

In a 2020 Safety at Sea/BIMCO survey, 31% of respondents indicated that their company had experienced a cyberattack, up from 22% the previous year. Respondents widely indicated that the COVID-19 pandemic had led to a higher dependence on digital connections and services, and that the level of digitization on ships was increasing; this was also identified as a growing vulnerability within the MTS. Despite the large number of ransomware attacks on the maritime industry in 2020, respondents identified phishing and malware as the most common attacks, and employees, spearphishing, and malware as the biggest cybersecurity threats.

Maritime Risk Management

Just as maritime cybersecurity is a specialized subset of the more general cyber discipline, maritime cyber risk management is a specialized subset of generic cyber risk management processes. In this context, risk analysis provides guidance to managers to develop security policies, create cyber risk awareness and training, select hardware and software, plan for personnel and staffing, create business continuity plans, and develop risk acceptance and management procedures. There are two primary forms of risk assessment, namely, *quantitative* and *qualitative*.

Quantitative approaches are objective and measurable. A classic quantitative approach would be to identify exploitable cyber vulnerabilities, determine the potential cost if the vulnerability were to be exploited, and estimate how often such an exploit actually occurs. In the formal terms of risk assessment, the cost of the exploit is the Single Loss Expectancy (SLE) and the frequency with which the exploit will occur each year is the Annual Rate of Occurrence (ARO). For a given vulnerability, the Annualized Loss Expectancy (ALE) is the product of the SLE and ARO.

Armed now with a list of vulnerabilities that require mitigation and their associated ALE values, defenses or security controls can be designed and put into place to decrease the SLE and/or ARO. After comparing the post-control ALE plus the cost of the controls with the pre-control ALE, managers can determine if the expenditures make sense and are necessary; if the cost of the defense is greater than the savings in ALE, the solution might well be rejected. As an example, spending \$15,000 on security controls to realize a \$9,000 saving in ALE probably does not make financial sense, while spending \$15,000 to save \$30,000 is probably a great idea.

Taking a strictly quantitative risk assessment approach to plan cybersecurity spending is a dangerous proposition. The first problem is accurately quantifying the SLE and ARO in the first place. The fact is, there is no truly accurate way to know the real costs of applying protections in cyberspace and it's easy to not spend \$15,000 if management can be convinced that the \$30,000 asset is not really at risk. Furthermore, it is nearly impossible to quantify intangibles such as reputation, customer and investor confidence, and the impact on supply chain partners.

A qualitative approach to risk assessment is subjective and indeterminate; it is, therefore, more flexible and, in some ways, more realistic, but not precise in terms of finances. The qualitative method is scenario-based, where planners describe events that can go wrong. For each *disaster scenario*, a score is assigned that typically describes the impact of the event to the organization and the likelihood of occurrence (Table 8.1). For each scenario, risk managers have to determine how to manage the risk in order to reduce the impact and/or frequency to an acceptable level. From this basis, contingency plans can be developed that include recovery systems, personnel, mutual aid, and more. This type of planning helps to identify strengths and vulnerabilities.

RISK ASSESSMENT MATRIX				PROBABILITY				
				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)				
				1=Extremely High 2=High 3=Medium 4=Low				

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

Table 8.1. Risk assessment matrix.

Qualitative planning for cyberdefense in the MTS combines knowledge of maritime systems and information threats per the Parkerian Hexad (see Chapter 2) in order to build maritime cybersecurity scenarios. Consider, as an example, scenarios related to cyberthreats to AIS. As Table 8.2 shows, there are a number of possible attacks on AIS, including GPS jamming, vessel spoofing, flooding, and creating a ghost vessel.

Each of these attacks can be categorized by the threat to information (e.g., jamming threatens the availability of information), the system or attack vector (e.g., AIS spoofing employs message injection), and the threat category (e.g., flooding is also a message injection attack).

Attack	Parkerian Hexad	Systems	Threat Category
GPS jamming	Availability	GPS/Jamming	Jamming
GPS failure/poor transmission	Availability	GPS	(nature, installation)
AIS device off	Availability	(human error)	(human error)
AIS malfunction	Availability	(nature)	(nature)
AIS bad data	Integrity, Availability, Utility	(human error)	(human error)
AIS jamming	Availability	Jamming	Jamming
AIS bit errors	Availability	(nature)	(nature)
Vessel spoofing	Integrity, Authenticity	Msg. injection	Msg. injection
Eavesdropping	Confidentiality, Authenticity	n/a	Eavesdropping
Flooding	Availability	Msg. injection	Msg. injection
Ghost vessel	Integrity, Authenticity, Utility	Msg. injection	Msg. injection
CPA/SART spoofing	Integrity, Authenticity, Utility	Msg. injection	Msg. injection
Disappearance	Integrity, Availability	Msg. deletion	Msg. deletion
AtoN spoofing	Integrity, Authenticity, Utility	Msg. injection	Msg. injection
Data diddling	Integrity, Availability, Authenticity, Utility	Msg. modification	Msg. modification
Weather spoofing	Integrity, Authenticity, Utility	Msg. injection	Msg. injection

Table 8.2. Risk assessment example: AIS.

Attack	Source	Likelihood	Severity	Ease
GPS jamming	A	4	2	3
GPS failure/poor transmission	H	3	3	n/a
AIS device off	A	4	1	1
AIS malfunction	H	5	1	n/a
AIS bad data	A	3	3	1
AIS jamming	A	5	2	3
AIS bit errors	H	3	3	n/a
Vessel spoofing	A	4	2	2
Eavesdropping	A	1	4	1
Flooding	A	4	3	3
Ghost vessel	A	4	3	3
CPA/AIS-SART spoofing	A	5	2	3
Disappearance	A	4	2	3
AtoN spoofing	A	4	2	3
Data diddling	A	3	2	3
Weather spoofing	A	4	3	3

Source: A = human-initiated attack, H = natural hazard

Likelihood: 1 = Frequent, 2 = Probable, 3 = Occasional, 4 = Remote, 5 = Unlikely

Severity: 1 = Catastrophic, 2 = Critical, 3 = Marginal, 4 = Negligible

Ease of attack: 1 = Trivial, 2 = Simple, 3 = Difficult, 4 = Very difficult

Table 8.3. AIS risk assessment.

These scenarios can also be mapped to a traditional qualitative threat matrix (Table 8.3). Continuing the example above, consider AIS vessel spoofing. This is a human-initiated attack; while it might be unlikely to occur, the severity of the attack is high, and it is a simple attack to initiate.

An alternative but similar approach to qualitative risk assessment uses two slightly different axes, namely, the value of the attack to the attacker and the ease of exploit. This is a different yet important shift in perspective on risk;

rather than focus on the impact of an attack on the victim, it takes into account the reward to the attacker. Clearly, an attacker is motivated to go after a high reward target and different types of attackers will place different value on different things. A hacktivist might be very happy with a defaced website, while a cybercriminal might settle for nothing less than a financial reward, and a nation-state might want something much more substantial or strategic. Although not explicitly described in these models, knowing something about the potential attacker—or potential award that a target offers—might assist in building a cyberdefense strategy.

Some sort of cyber risk assessment process is essential for an organization to determine its own risk exposure and risk appetite. There are four ways to manage risk:

- *Accept*: If the risk is low enough or hazard unlikely enough, accept the risk and possible consequences.
- *Avoid*: Do not perform an activity that involves more risk than is acceptable.
- *Reduce/Mitigate*: Employ policies and procedures (including defensive countermeasures) that can control the level of risk or decrease the impact of an event.
- *Transfer*: Move the risk to a third-party, e.g., buying insurance, leasing rather than owning equipment, or outsourcing certain activities.

Maritime Cybersecurity Guidelines and Organizations

Understanding maritime cyberthreats, vulnerabilities, and risks is the basis for an organization to prepare the cyber policy and procedure documents that guide equipment purchases, network architecture and configuration design, staffing, training, service agreements with telecommunications carriers and vendors, supply chain partner policies, and other related functions and tasks. Policies and procedures guide day-to-day activities; organizations also need incident response procedures, contingency plans, and business continuity processes.

Proper cybersecurity planning is a big task. This section provides a high level introduction to some of the framework documents available to the maritime industry to aid in developing cyberdefense policies and procedures, as well as some of the industry and government groups providing cyber assistance to the MTS.^[23]

Policy and Procedure Framework Documents

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)^[24]

As mentioned earlier in this book, the NIST Cybersecurity Framework has emerged internationally as a common reference for a large number of cyberdefense guidance and best practices recommendations. The framework can be used as a template with which to create profiles of functions, categories, subcategories, and recommended practices that are relevant to particular organizations or tasks. The U.S. Coast Guard, for example, has adopted maritime cybersecurity profiles related to bulk liquids transfer, offshore operations, passenger vessel operations, and the Department of Energy's Cybersecurity Capability Maturity Model (C2M2).

NIST also has a series of special publications devoted to security of information technology systems. The SP 800-series covers a variety of topics of interest to the maritime industry, ranging from industrial control systems and cryptography to IoT and e-mail.

BIMCO^[25] ET AL. INDUSTRY CONSORTIUM

A consortium of more than 20 maritime companies and organizations, including the Baltic and International Maritime Council (BIMCO), the International Chamber of Shipping, the International Union of Marine Insurance, and the World Shipping Council, released version 4 of its guidelines for shipboard cybersecurity in 2020. Its goals are:

- Establish awareness of the safety, security, and commercial risks associated with inadequate cybersecurity protections
- Protect shipboard IT infrastructures and the data used in the ship environment
- Manage and control IT users' access to information
- Manage communication between ship and shore
- Develop and implement a cyber incident response plan based on a risk assessment model (Figure 8.1)



Figure 8.1. BIMCO Cyber Security Awareness risk management cycle.

BIMCO followed up this plan with a new contract clause requiring that signatories address cybersecurity risks and incidents that might affect their ability to fulfill their obligations to their contract partners. This clause will require contracted parties to have cybersecurity policies and procedures in place, have the ability to respond quickly to cybersecurity incidents, and notify the other party in case of a cyber breach.

INTERNATIONAL MARITIME ORGANIZATION (IMO)^[26]

The IMO is an agency of the UN. It is not a standards organization, per se, but develops a regulatory framework for international shipping that addresses safety, environmental concerns, legal issues, security, and international technical cooperation. IMO is, perhaps, best known for the SOLAS Convention, adopted in 1914 after the sinking of TITANIC, and the International Convention for the Prevention of Pollution From Ships (MAROL), first adopted in 1983.

While the IMO has not produced any detailed cyberdefense specifications for the maritime industry, its guidance documents are intended to support safe and secure shipping that is operationally resilient to cyberthreats. The primary IMO cybersecurity documents are a set of high level recommendations to protect shipping from current and emerging cyberthreats and vulnerabilities. These guidance documents describe vulnerable shipboard systems including bridge systems, cargo handling and management systems, propulsion systems, and communication systems, and describes the risk management steps to employ when building cyberdefenses. The recommendations also note that IT and OT systems have different purposes and characteristics, leading to mention of automation on board ships. While this document does not directly address autonomous vessels, the IMO has produced guidelines that address safe, secure and environmentally sound Maritime Autonomous Surface Ships (MASS) operations.

In 2017, the IMO Maritime Safety Committee (MSC) adopted a resolution encouraging maritime administrations to

ensure that cyber risks are appropriately addressed in existing maritime safety management systems. Known as IMO 2021, the resolution included a set of Maritime Cyber Risk Management recommendations that IMO encouraged shippers to implement no later than the first annual verification of a vessel's Document of Compliance in the year 2021. Some maritime administrations and insurance companies are requiring adherence to IMO 2021.



Figure 8.2. ABSG top-down cyber management approach.

AMERICAN BUREAU OF SHIPPING (ABS)^[27]

The ABSG Consulting CYBERSAFETY® maritime cyber guidance document takes a top-down approach to risk management. The ABSG framework (Figure 8.2) is built around a set of baseline tasks that should be part of a maritime organization's existing cyberdefense strategy, organized in three categories: practices and processes (Tasks 1-3), risk management (Tasks 4-6), and resource and asset protection (Tasks 7-9). Tasks 10-23 describe an additional 14 advanced capabilities in these same three categories, adding a depth and breadth to the organization's cyberdefense implementation, including cyberdefense standards, threat intelligence, vulnerability assessment, and system testing.

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)^[28]

ENISA provides cybersecurity recommendations and workshops, supports policy development and implementation, and collaborates with operational cyber teams throughout Europe. While it does not have a specific maritime role, ENISA has provided two recommendations related to the MTS.

In 2011, ENISA produced the first report in Europe detailing cybersecurity challenges in the maritime industry. While in some sense dated, the recommendations and insights are interesting to read, notably because this era was experiencing both increased dependence upon ICT and new, emerging OT systems, all under the shadow of the Stuxnet attack and software threats to hardware.

ENISA is also one of a handful of agencies to produce recommendations for port cybersecurity. Their report identifies the stakeholders at a port and the information flows between them. The recommendations include a taxonomy of port assets and a catalog of cybersecurity threats to, and challenges for, ports. The report also offers a suite of policies, organizational practices, and technical measures that can be used to address cyberthreats.

INSTITUTION OF ENGINEERING AND TECHNOLOGY (IET)^[29]

The IET is a multidisciplinary engineering professional society in the U.K. Like ENISA, IET does not have a specific role in maritime standards, although it has two best practices guides related to maritime cybersecurity.

The IET's guide to cybersecurity for ships is a management framework intended for board members, insurers, ships' senior officers, and managers of IT and OT systems of any ship-owning/operating organization. The port cybersecurity guide is intended for managers responsible for the cybersecurity protections of ICT systems at a port and for the vessels docked at a port. Both guides provide the steps for preparing a cybersecurity assessment, developing a cybersecurity plan, and managing cybersecurity within the organization.

INTERNATIONAL ASSOCIATION OF PORTS AND HARBORS (IAPH)^[30]

The IAPH is a global alliance representing more than 300 ports and port-related organizations in 90 countries. It is a non-governmental organization (NGO) with consultative status to the IMO and several other UN agencies.

IAPH released version 1.0 of its cybersecurity guidelines for port facilities in 2021. The document's stated target audience is executive decision makers at ports. The guidelines are largely non-technical in nature, where the first half of the document provides a broad coverage of cyber risk management in the maritime sector. The remainder of the document describes some technical cyber countermeasures, information sharing in the industry, workforce training, incident response and recovery, and process improvement.

U.S. COAST GUARD (USCG)^[31]

The U.S. Coast Guard is an agency in DHS. USCG has a unique role in the U.S. military, having a law enforcement function in both U.S. and international waters, and a federal regulatory function. USCG functions also include search and rescue, security throughout the MTS, drug interdiction, port facility inspection, maintenance of aids-to-navigation, and fishery regulation enforcement.

The Coast Guard has broad regulatory oversight over vessels and maritime facilities in the U.S. and U.S. waters, and has two primary roles related to cybersecurity. First, it must maintain the security of USCG ICT assets, including systems and networks used to manage and maintain Coast Guard operations and shipboard systems. Second, it assists in the cyber protection of information assets throughout the MTS, including at port facilities and on civilian vessels. CGCYBER is a part of the DoD's U.S. Cyber Command (USCYBERCOM), primarily for external facing threats and attacks, while its internal mission is the preparation of its own cyber workforce.

USCG's initial cyberstrategy, released in 2015, was primarily focused on its own cyber requirements. The three overall strategic goals were to build secure and resilient IT systems in order to defend cyberspace and ensure the USCG's mission; enable operations in cyberspace by detecting, deterring, disabling, and defeating adversaries; and protect the MTS infrastructure, which includes ports and terminals, ocean carriers, near coastal shipping, and Western Rivers and the Great Lakes. The plan also recognized that long-term success required recognition of cyberspace as an operational domain, information sharing among maritime stakeholders, the creation of a qualified cyber workforce, and leveraging partnerships with MTS stakeholders.

The USCG strategic outlook for maritime commerce, released in 2018, addresses cyber aspects of the maritime domain in more detail. This document speaks to the fact that increased use of ICT, communications, and OT in the maritime industry results in a broader threat profile and attack surface in cyberspace. The outlook also foreshadows the increased dependence of maritime systems on GPS and the growing challenge of spoofing events. The future-looking document draws a direct line between cyberthreats and the long-term economic health of the maritime sector.

The Coast Guard's vision to protect and operate in cyberspace was updated in 2021 with its *Cyber Strategic Outlook*. This document identifies three lines of effort in cyberspace. First, USCG needs to defend and operate a secure, resilient Enterprise Mission Platform (EMP), its portion of DoD's Information Network (DODIN). Second, USCG's role in protecting the MTS extends into cyberspace, where existing frameworks, standards, and best practices will be employed to identify, prevent, and respond to cyber incidents. This role will encompass USCG assets from the Captains of the Port to USCG intelligence capabilities. Finally, USCG remains committed to employing advanced cyber capabilities in order to operate in and through both cyberspace, as well as its more traditional operational domains.

The Coast Guard has regulatory authority for the security of near coastal and outer continental shelf maritime facilities, all covered under the Maritime Transportation Security Act (MTSA) of 2002. USCG guidelines describe cyber risks at MTSA-regulated facilities and include requirements for, among other things, a facility security assessment and operational plan, security administration and organization, personnel training, drills and exercises, communications, interfacing with vessels, security systems, and a variety of security measures. Not surprisingly, the USCG guidelines reference the NIST framework.

In the last few years, USCG has introduced several initiatives to improve their cyberdefense posture and service to the MTS, including:

- Establishing deployable Cyber Protection Teams that can offer response to real-time cyber incidents
- Creation of a cybersecurity subcommittee for each of the 41 Area Maritime Security Committees (AMSC), to advise about relevant maritime cybersecurity issues
- Assigning an MTS cybersecurity specialist at each sector to take the lead in cyberdefense issues for both USCG and civilian MTS stakeholders
- The creation of a Cyber Systems major at the USCG Academy to help prepare the next cadre of officers

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)^[32]

The Cybersecurity and Infrastructure Security Agency is an agency within DHS tasked with protecting U.S. federal networks (the .gov domain) and building the nation's capacity to understand, manage, and respond to cyber and physical risks within the nation's critical infrastructure sectors. CISA is also tasked with guiding public sector cybersecurity strategies by enhancing cyberdefense across all levels of government, coordinating state cybersecurity programs, and improving the government's ability to repel cyberattacks (ranging from ransomware to attacks on the supply chain). CISA is not an enforcement agency nor does it have an enforcement branch; instead, it focuses on risk management and, working with public and private sector partners, shares threat intelligence and builds a more cyber resilient infrastructure. CISA's Cybersecurity Branch addresses a number of physical and cyber threats, including ICS/OT and cyber-physical system security.

One of the domains for which CISA has responsibility is the Transportation Systems Sector (TSS). CISA has defined a cybersecurity framework describing a risk management approach to finding cybersecurity vulnerabilities and using this information in conjunction with the NIST Framework.

CISA also oversees the Maritime Modal Sector Coordinating Council (SCC), chartered with coordinating the preparedness and response capability between the U.S. MTS and government agencies. CISA's other activities pertinent to the MTS include the development of ICS security mechanisms and operation of the ICS Joint Working Group (ICSJWG). CISA's U.S. Computer Emergency Readiness Team (US-CERT)^[33] is a public service for cybersecurity information sharing and vulnerability alerts. CISA has also produced a series of Cyber Resilience Review guides to assist organizations in a self-assessment of their cyberdefense posture so that they can spot and fix weaknesses in their planning.

CISA's Cyber Security Evaluation Tool (CSET[®]) provides individual organization of any size to do a cybersecurity self-assessment. CSET employs a systematic, four-step process, including the tools, so that an organization can select one or more relevant cybersecurity standards, answer a set of questions to determine their appropriate security assurance level, create a network topology diagram, and review an automatically-generated report with recommended best practices and/or any identified gaps in cybersecurity protections.

Industry Groups

Other industry groups provide training, cyberattack response services, and best practices guidance to the maritime industry. One group of organizations provides information sharing. The Clinton Administration, in 1997, identified the nation's critical infrastructure sectors as potential targets requiring protection, and called for the creation of public-private information sharing entities. Since that time, several dozen information sharing and analysis centers/organizations (ISACs/ISAOs) have emerged to help the various sectors and interest groups share information and understand the ramifications of cyber incidents on their community. Among these groups aiding the maritime sector are:

- *Maritime Information Sharing & Analysis Center*: Operating as a part of the Maritime Security Council, the Maritime ISAC provides information sharing services to shipping lines, ports, cargo handlers, and others in the MTS. Their focus is on physical security rather than cyber.^[34]
- *Maritime & Port Security Information Sharing & Analysis Organization (MPS-ISAO)*: An organization with a mission to form strategic private-public partnerships to advance maritime cyber resilience. MPS-ISAO provides threat intelligence reports and advisories to vetted members of the maritime community, and additional information sharing services and resources to ISAO

- members.^[35]
- *Maritime Transportation Sector Information Sharing & Analysis Center (MTS-ISAC)*: An organization with a mission to improve cyber risk management across the entire MTS community, and to promote and facilitate maritime cybersecurity information sharing, awareness, and training. The organization also supports collaboration efforts between private and public sector stakeholders.^[36]
- *Operational Technology Information Sharing & Analysis Center (OT-ISAC)*: An information-sharing community across the OT sector, where stakeholders can securely and anonymously share information. Although not specific to maritime issues, there is a large overlap between OT interests and the use of OT within the maritime sector.^[37]

Classification (or class) societies are NGOs that establish technical standards related to the design, construction, and operation of ships and offshore structures. The primary focus of class society standards are a ship's hull, propulsion and steering systems, power generation, and other systems related to a vessel's operation. Class societies employ a program of inspection and certification to provide a baseline reference point on ship safety and reliability for ship builders, brokers, operators, flag administrations, insurers, and the financial community.

The International Association of Classification Societies (IACS) has a dozen member organizations, including the American Bureau of Shipping (ABS, U.S.), Bureau Veritas Group (BV, France), China Classification Society, Lloyd's Register (U.K.), Nippon Kaiji Kyokai (ClassNK, Japan), and the Russian Maritime Register of Shipping. Relevant IACS cyber guidelines include IACS Recommendation 166 addressing cyber resilience and IACS Requirement E22 for onboard use of programmable electronic systems.

Bureau Veritas Group^[38] is a private company, formed in 1828, that specializes in testing, inspection, and certification in a variety of sectors, including building and infrastructure, agriculture and food, industry, maritime and offshore operations, and consumer products. BVG's maritime initiatives include:

- The SW-Registry notation, which acknowledges an organization's software change management process. The notation requires the creation and maintenance of a certified database of software used on board a ship, and is used to ensure that new software versions are properly tracked. This type of software management allows ship owners to comply with IACS Requirement E22.
- The SYS-COM notation, which addresses cybersecurity and the prevention of malicious cyberattacks. SYS-COM consists of voluntary guidelines for data exchange between ship and shore.
- BVG Guidance Note NI 641, which provides recommendations for securing autonomous vessels. NI 641 describes general considerations for autonomous operation, a risk and technology assessment plan, and a review of the functionality and reliability of autonomous systems.
- BVG Rule NR 659, which offers guidance for securing vessels that employ IT and OT systems, applies to the design, construction, and maintenance of these computer-based systems, and enables smart shipping. In 2020, ELISA LARUS became the first liquefied natural gas (LNG) carrier to receive the BVG's cyber security notation, which also complies with the IACS 166.

Nippon Kaiji Kyokai, more commonly known as ClassNK,^[39] is a non-profit classification society based in Japan. The focus of ClassNK's work is to protect life and safety at sea, and prevent pollution of the maritime environment. Its guidelines for cybersecurity on board ships includes a framework for implementing cyberdefense controls for traditional computer-based systems and ICS-automated systems, and aligns with IACS 166. ClassNK will provide cybersecurity verification during the design and construction stages of new ship builds. In 2021, ClassNK launched a collaborative project with the Panama Maritime Authority on a voluntary cyber incident reporting system and analysis program. Panama is the world's largest flag state.

In 2018, Wärtsilä and Templar Executives opened the International Maritime Cyber Centre of Excellence (IMCCE) in Singapore, touted to be the first such maritime cybersecurity center in the world. IMCCE programs are intended to help the maritime industry maintain cyber awareness and incident response. The Maritime Cyber Emergency Response Team (MCERT) is an international cyber intelligence and incident support platform, offering real-time assistance to its members in case of cyberattacks and incidents. The Cyber Security Reporting Portal (CSRP) provides a mechanism for its members to report cyber-related issues. A Cyber Academy will offer a range of cybertraining, from coaching senior management to cyber awareness for all employees of an organization.

Maritime insurance dates back to 1686 when policies were offered in Edward Lloyd's Coffee House in London. The coverage framework for ships and cargo is among the most mature in the insurance industry, and addresses damage or loss to vessels, terminals, cargo, and passengers. Marine insurers generally require compliance with cyber safety guidelines issued by class societies, IMO, and/or regulatory agencies; some insurers require that a

vessel has a class society certification or demonstrate compliance with IACS Recommendation 166. The future of cyberinsurance is an area of some controversy and concern since insurance companies such as Lloyd's of London and Zurich have included cyberwar exclusions in their policies.

Conclusion and Summary

This chapter introduced organizations, agencies, and resources that assist maritime entities to develop and implement a cybersecurity plan. It is not an exhaustive list and we have purposely not mentioned commercial companies providing maritime cybersecurity products and services, as that is well beyond the scope of this discussion.

There is no one-size-fits-all approach to cyber planning. All ports, ships, shipping lines, manufacturers, and other MTS stakeholders are similar, but different; so too are their cybersecurity needs and cyberdefense implementations.

The next—and final—chapter of the book brings together concluding thoughts, ideas, and suggestions about cyberdefense in the maritime sector.

Chapter 9: Concluding Thoughts

Introduction

Our discussion about cybersecurity and our presentation of cyberattack case studies might seem to paint a bleak picture. The intention is not to make the reader despair, but rather to raise their awareness of the challenges that face the maritime community. “Chance favors the prepared mind”^[40] says a lot about our approach. This chapter offers some concluding comments, advice, observations, and suggestions.

Cybersecurity is complicated, and maritime cybersecurity is particularly complex. Panelists at the Maritime CEO Forum in 2018 observed that shipping is between 30 and 500 years behind in technology. Seafaring has a history going back thousands of years and with that comes a certain inertia that is hard to change. Indeed, we live in an era of autonomous vessels, while we are still using bills of lading that have not changed significantly in centuries.

Cyberdefense is a new paradigm of thinking in the maritime domain. Executives and managers within the MTS need to take a systems approach, proactively managing networks and sharing information within the industry. The maritime sector’s safety culture needs to meet the reality of information security; it is not a simple task, but it is an essential one. The phrase “herding cats” is often applied to difficult management situations within an organization; with cybersecurity, it is finding the right balance of protection and productivity, and getting the entire user community to comply with necessary security directives. Maritime cybersecurity management issues are somewhat exacerbated by the large number of moving vessels (each an independent ICT network), the ability for one vessel to touch many ports, and the fluid nature of some crew members. If herding cats is difficult, herding fish is a somewhat more applicable metaphor (Figure 9.1).



Figure 9.1. The first author’s wife herding fish in Hawaii.

In December 2020, the U.S. White House released the National Maritime Cybersecurity Plan (NMCP). This document is a clarion call about the pressing need for cybersecurity protection for the MTS and recognizing the importance of maritime to no less than the food, energy, economic, homeland, and national security of so many countries. The NMCP also indicated three main thrusts required to address the problem: identify risks and standards, engage in intelligence and information sharing, and build a maritime cybersecurity workforce.

Basic Principles

Although the MTS has some unique cybersecurity attack vectors, planning a maritime cyberdefense posture starts with basic principles. At a high level, consider these 10 information security principles for managers in the maritime industry:

1. Don't be in denial about the problem.
2. Don't underestimate the problem.
3. Don't be hostile to government and regulators.
4. Don't make cyberdefense an issue buried in bureaucracy.
5. Don't attempt to defend the entire network all at once; identify the crown jewels and prioritize your cyber assets.
6. Do participate in industry information sharing.
7. Do sponsor industry research and development initiatives.
8. Do think holistically.
9. Do look at worst-case scenarios.
10. Do have an industry strategy.

For users and maritime computer system managers, a majority of cybersecurity problems can be alleviated by simply following good cyberhygiene and adhering to elementary "Cybersecurity 101" best practices:

- Use strong passwords and two-factor authentication.
- Carefully monitor employee movements and transfers. Delete accounts for individuals who should no longer have access to a system.
- Employ individual profiles and passwords; do *not* use generic accounts.
- Minimize use of administrative accounts and privileges.
- Assign user access rights only on an as-needed basis; employ Zero Trust practices where appropriate.
- Audit the network to know what hardware is connected and what software applications are installed.
- Segment shipboard networks into isolated subnets, where possible.
- Keep software patched and up-to-date.
- Train users to create a cybersecurity safety culture.
- Back up critical systems.
- Employ anti-malware software and other defense in depth strategies.
- Be wary of external media.
- If you don't know, ask.

Cybersecurity defenses are often described in terms of *defense in depth*, meaning that you cannot rely on any single approach to protect your cyber assets. Just as a village might be protected by a castle's high walls, a moat, and flat open ground, our ICT and OT infrastructure needs a layered approach to defense. The outermost layer is generally physical, using mechanisms that keep unauthorized people away from systems. The second layer is logical, using a network architecture that segregates devices onto different functional networks. The final layer is to harden each individual system. This is the purpose of having security policies, procedures, training, and in-house exercises.

In the preface to this book, we offered a scenario about the LADY P, a ship showing signs of being at risk due to a cyber compromise of several of its automated systems. The U.S. Coast Guard has already sent cyber boarding teams to assist vessels stricken with cyber issues, as first reported in 2019 with a deep draft vessel entering the Port of New York and New Jersey. Many of the points above are derived from USCG Marine Safety Information Bulletins (MSIB). Maritime authorities around the world increasingly take these types of events seriously and are starting to consider the cybersafety of a vessel to be as important as having the proper number of life jackets and a working fire suppression system onboard.

Indeed, maritime stakeholders need to approach cybersecurity as a safety issue. The best prepared organizations view cyber risks at the same level as other risks to the enterprise and manage cyberdefense with a view to the impact on the business. Conversely, poorly prepared organizations delegate cyberdefense to the IT staff, who generally take a technology approach rather than a risk management approach.

Risk Management, Revisited

We discussed qualitative and quantitative risk assessment in the previous chapter. As mentioned earlier, a quantitative approach uses the cost of a cybersecurity incident (Single Loss Expectancy) and the frequency with which we think that event will occur (Annual Rate of Occurrence) to calculate an Annualized Loss Expectancy. We then plan a mitigation strategy and compute the cost. In a classic cost-benefit analysis, we would compare the first-year ALE-without-mitigation to the sum of the second year's ALE-with-mitigation plus the mitigation costs; if the

second-year's cost is less, we have a good solution, and if the cost is more, we might just accept the cost of the incident.

This attempt to use a cost-benefit analysis to determine return on investment (ROI) is common in business environments but does not translate well for justifying cybersecurity spending. The first problem is accurately quantifying the SLE and ARO. The fact is, we don't actually know the real costs of protecting ourselves in cyberspace, and it is difficult to accurately quantify the asset value of intangibles such as reputation, customer and investor confidence, and the impact on supply chain partners.

Cybersecurity, however, is not a tangible asset and, therefore, should not be evaluated as an investment. Think, instead, in terms of the return-on-negligence (RON), or the cost of doing nothing. By way of example, consider the Year 2000 (Y2K) problem in the late 20th century. The Y2K problem was fundamentally an issue of poor programming practices; programmers had written code for many decades using only the last two digits of the year instead of all four.^[41] There were fears in the late 1990s that the power grid might fail, the Internet would crash, some software would stop working, and other doomsday events might occur when the year 1999 rolled over to 2000. Hundreds of millions of person-hours and an estimated \$300 billion was spent to mitigate Y2K. And then... nothing bad happened on January 1, 2000. This was because we were prepared. But, soon thereafter, many pundits in the computer industry and social commentators started to argue that we had spent too much to fix Y2K and their evidence was, in essence, *since nothing bad happened, we obviously spent too much on the solution*. They were, in effect, trying to quantify how much we overspent protecting our cyber assets.

We cannot apply that type of thinking to defending ourselves in cyberspace. Defending information and cyberspace today is even more important and critical than it was 20 years ago. What is the cost of doing nothing about cyberdefense? No company, of course, wants to be a headline for the wrong reason. But in addition to embarrassment and a possible decline in customer confidence, consider that the loss of intellectual property can put a company out of business due to the loss of critical trade secrets. And, most significantly, consider the potential impact on a shipping company or port if a cyberattack causes the death of passengers, crew members, dockworkers, or others.

There are also very real tangible costs of a data breach, particularly as maritime organizations hold an increasing amount of PII, PHI, and sensitive personal information (SPI) for employees, contractors, and passengers. According to the California Consumer Privacy Act (CCPA), for example, consumers may be able to sue the holder of private information up to \$750 for each breach of privacy, while the state attorney general can sue up to \$7,500 for each incident of intentional privacy violations. The CCPA applies to companies doing business in California that gross at least \$25 million, which would clearly include most maritime shipping lines as well as the large ports in that state. The EU's General Data Protection Regulation (GDPR) can place huge fines on any incident of private data loss that is judged to be due to non-compliance with the regulation, particularly if a breach can be shown to be due to negligence or the company has a history of personal data infringements. These fines can be up to €20 million or 4% of the company's global annual revenue.

"No man is an island,"^[42] the poets say—nor are any of the world's cyber environments. Thanks to a ubiquitous, high-functioning, globally accessible network, and an increasingly mobile user base, every cyber asset on the planet is connected, one way or another, to every other, thus making the potential for a cyberattack to reach far beyond its intended target. Being a responsible employee by exercising thoughtful cyberhygiene goes well beyond an employee's company. Taking the right steps—or not—can have global implications.

The risk management approach to cyberdefense is a much better approach than one trying to justify expense using ROI. An organization does not need to spend an infinite amount of money on cybersecurity, but must think deliberately about its cybersecurity plan. As Leaders and Managers, ask questions such as: "What are our cyber assets and where are the potential vulnerabilities?" "What is the likelihood of a vulnerability of a particular asset being exploited?" "What is the potential impact of such an exploit?" One does not have to quantify these answers; in almost all cases, they can't be accurately quantified anyway. But the answers can be used as a tool to triage assets and vulnerabilities, so that protection can be directed to the most important ones first. You can't do everything at once, so make an orderly plan. And continually review, update, test, and modify the plan, as necessary.

There is an old adage that there are no secure sites on the Internet, only vigilant ones.^[43] The MTS is very much connected to the Internet and needs the same watchfulness. Vigilance requires people to know what to do and to do their job defending cyberspace correctly, starting with the end users. And cyberdefense is not solely a technology solution. There is another saying: "Anyone who thinks that technology can solve their problem does not understand technology or their problem."^[44]

Finally, do not fall prey to the age-old trap of allowing complacency to set in. In the world of cybersecurity, complacency kills. The words of Peter Senghe ring true here: "Intelligent people tend to espouse theories of action

that have little to do with actual behavior.”

Resilience

The primary theme of this book has been about securing and defending information systems from attack. In this context, *resiliency* refers to an ICT and OT system’s capability to recover from failure and continue to operate even while under attack. In cyberspace, much more than in real space, reasons for failure tend to be due to the actions of people rather than the “natural” failure of software and hardware. Thus, while the system may have built-in resiliency, that fault-tolerance might not be protecting from the correct adversary.

The *Plug into the Formula Maxim*, introduced earlier in this book, says, in part, that engineers and system designers “view nature or economics as the adversary, not people, and instinctively think about systems failing stochastically, rather than due to deliberate, intelligent, malicious intent.”

Consider the problem that Maersk endured with the WannaCry worm. Maersk had backups for their data but did not backup their Active Directory (AD) servers. The AD system in an enterprise network has built-in fault-tolerance; if an AD server fails, it is merely taken offline. When a new AD server is added to the network, it is populated with necessary data by exchanging information with the other AD servers. What the network is not prepared for is losing all of the AD servers at once. This is also true of the Internet’s Domain Name System (DNS).

Similarly, GNSS systems are designed to handle the loss of a satellite or two due to natural causes. When there is a failure, the satellite is taken offline and a backup satellite moved into position. None of the GNSS are designed to recover from the near-simultaneous failure of most or all of the satellites in the constellation, a distinct possibility with today’s available anti-satellite technology and open threats against satellite-based navigation.

Users and User Training

It is common in security circles to state that users are the weakest link in the defensive chain. Many cybersecurity papers, Web blogs, conference presentations, and corporate studies focus on this phenomenon—so many that the human weak link is sometimes accepted as an immutable fact. Yet, we cannot take the view that successful cyberattacks are inevitable due to our users.

While people are one of the most common cyberattack vectors—think social engineering—people also design critical ICT and OT systems, as well as cyberdefenses. Blaming the user for poor cybersecurity makes the false assumption that vendors are providing secure systems in the first place. Consider the flaws in our underlying operating systems and applications, hard-to-configure software and hardware, obtuse user manuals, and complex human-machine interfaces, coupled with inadequate training.

Another example comes from the world of AI. When the technology began to be deployed commercially, many industry pundits heaved a sigh of relief over the fact that critical decision-making would now be free of human bias. Wrong: people write AI algorithms, and inherent in that activity is the deliberate or inadvertent inclusion of human bias.

No OS is completely secure and no developer can patch all software vulnerabilities during every patch cycle; indeed, there is a huge arsenal of zero-day exploits just waiting to be launched for which there are no protections. Software constantly undergoes updates and patching, making the uniform distribution of the latest up-to-date version difficult within a large enterprise system. A communications protocol or encryption scheme might be secure on paper, but then have flaws in the implementation. Secure computers and networks are often undermined by the mismanagement of passwords and encryption keys. These vulnerabilities are not created by users but are intrinsic to any system designed and operated by humans.

A proper cyberdefense is difficult and we are reminded of the adage, “No battle plan survives first contact with the enemy.”^[45] That said, boxer Mike Tyson’s version, “Everyone has a plan ‘till they get punched in the mouth,” may sound more relevant in the context of cyberattack.

These issues are exacerbated within the complex digital environment that is the MTS. Ships’ crews and dockworkers may have varying levels of cybersecurity awareness and may not be fully integrated into a cybersafety culture. There is a critical need in the MTS to conduct more cybersecurity training, education, table-top exercises, and certification for the MTS and its operators.

There are some pundits that claim that user cybertraining is wasted, evidenced by the fact that social engineering—that is, an attack on people—remains a bigger problem in the MTS than attacks on computer systems. What this demonstrates is that routine, perfunctory annual cybertraining is failing—which it has been for the last 30 years. Yet, just as we train crews to fight fires, which they do very effectively when the need arises, we can and must train every member of the MTS to be cyberaware. We need ship’s officers and professional mariners that are cyberaware.

The training must be active, engaging, and practical, including exercises that involve anyone with access to information or a computer. This practice might be costly and time-consuming—but the cost of doing nothing is unacceptable.

Threats, Vulnerabilities, and Exploits

Cybersecurity is an ever-evolving field. New vulnerabilities in cybersystems do not just appear as new hardware and software is released; sometimes a vulnerability has been in existence for many years, but no one found or reported it—or created an exploit—until the point at which a patch was released.^[46] The threat landscape is always in flux and is very dynamic. Indeed, there are already exploits for some technologies that have not yet been widely deployed, which means that the Bad Actor community is just waiting for the enabling vulnerabilities to catch up. For example, AIS weather report messages can be spoofed. This is not a major problem at this time because most mariners do not receive AIS weather messages—yet. The point is that our cyberdefense mechanisms must address today’s vulnerabilities and exploits, and anticipate tomorrow’s.

Finally, threats must be put into context. Figure 9.2 shows the light configuration of a vessel that you do not want to see at night—a minesweeper engaged in minesweeping activity coming in your direction. Not only is this ship coming directly at you, it suggests that you are already in very dangerous waters, per Rule 27(f) in the COLREGS.

While this portrayal has a certain element of dark humor to it, there is also a real-world analogy. When a ship is in a minefield, what is the real problem? Is it the threat of hitting a mine or is it the vulnerability of the ship to the damage caused by the explosion?

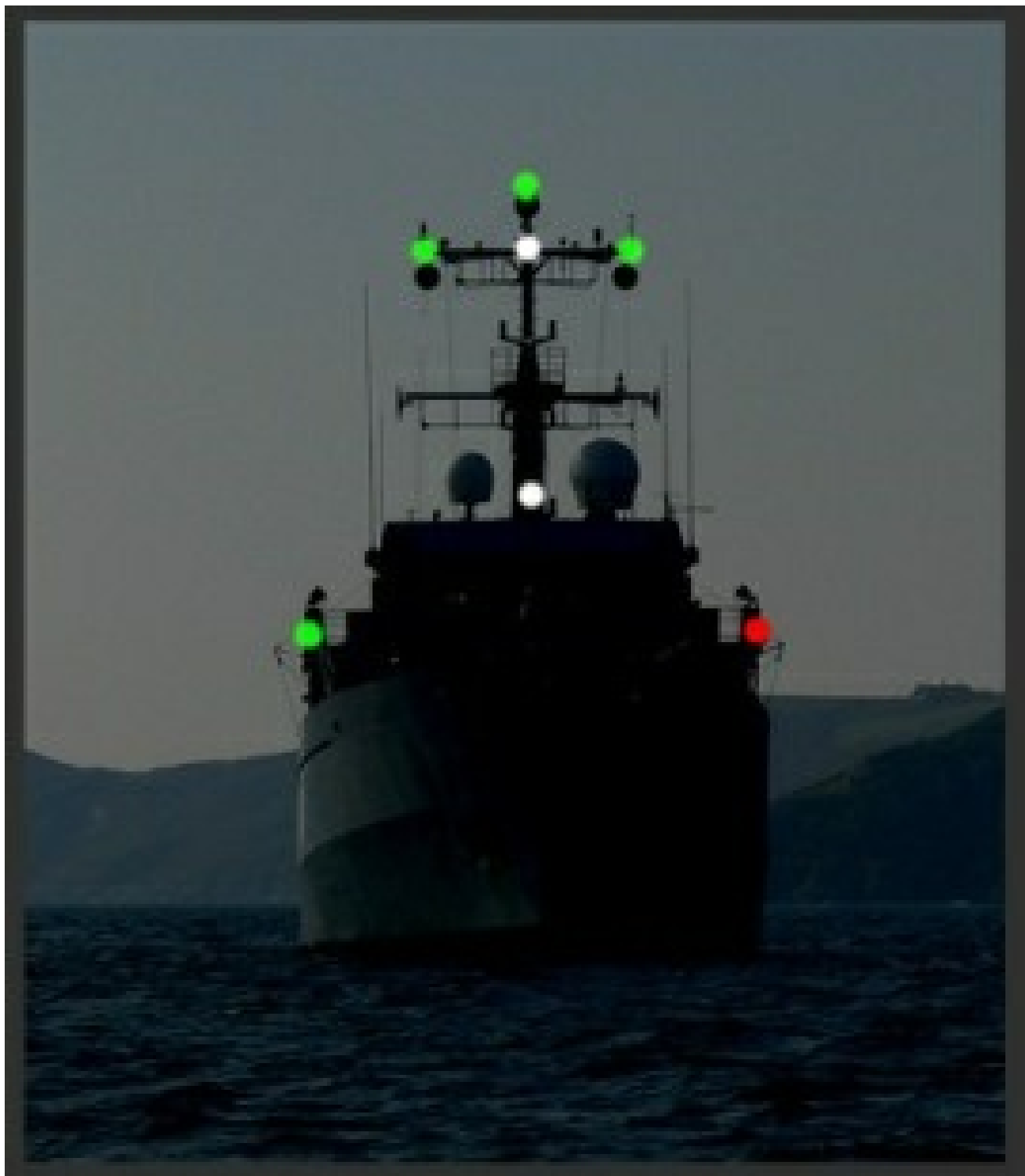


Figure 9.2. Something you don’t want to see at night.

During the early days of the Battle in the Atlantic during World War II, Germany deployed magnetic mines against the British. The mines rose from the seafloor when they detected the small change in the Earth’s magnetic field that occurred when a steel-hulled vessel came within range. The British, upon discovering this mechanism, took countermeasures to degauss (i.e., demagnetize) their warships. This change eliminated the exploit due to the ship’s disturbance of the magnetic field and, at least temporarily, obviated the threat; the vulnerability of the ship to a mine

was not eliminated but the exploit was mitigated. In cyberspace, we can't control where the mines are, but we can control our susceptibility to getting hit by one and the subsequent damage that could result.

This leads to the following general truth about cybersecurity:

Vulnerabilities Trump Threats Maxim: If you know the vulnerabilities (weaknesses), you've got a shot at understanding the threats (the probability that the weaknesses will be exploited and by whom). Plus, you might even be OK if you get the threats all wrong. But if you focus mostly on the threats, you're probably in trouble.

Threats are a danger from someone else that can cause harm or damage. We might or might not be able to identify a potential threat, but we cannot control them. *Vulnerabilities* are flaws or weaknesses in our own systems that can be exploited by a threat actor. Indeed, not all vulnerabilities can be exploited. We are—or should be—able to identify our vulnerabilities and correct them.

While we cannot control the threats, we should be knowledgeable about the threat landscape and have an idea of threat actors who might wish to do us harm, but we should not obsess over the threats while planning a cyberdefense. Instead, we should look inward at our own systems, seek out the vulnerabilities, and plug the holes. New threats will emerge over time, but that doesn't change our plan to fix our vulnerabilities.

Ironically, there is a corollary to this maxim: "Identifying threats can help get you funding while identifying vulnerabilities probably won't." Almost all cybersecurity professionals have gone to management and sought funds for an emergency update to some hardware or software, just to be told that fixing a vulnerable system can always wait until the next budget cycle. Conversely, show management a memo from IMO or USCG, or a warning from an ISAC/ISAO, that highlights a credible threat directed at that same hardware or software, and funds will become available.

Conclusion and Summary

"The race is not always to the swift, nor the battle to the strong, but that is the way to bet." (Damon Runyan, 1880-1946)

We can summarize the subject matter in this book as follows:

- The maritime transportation system is complex.
- The entities within the MTS are inextricably intertwined.
- There are a large number of attack vectors in cyberspace.
- You cannot control all parts of the network, and fragmentation in the industry makes it difficult to adopt new technologies.
- You need organized response, contingency, and business continuity plans.
- Cybersecurity problems are real, and the threat landscape is constantly changing.
- Cyberthreats can be mitigated, not eliminated.

Given this, we recommend that maritime organizations take an *all-hazards approach* to cybersecurity and cyberdefense. This means that organizations should not dwell on threats and the cause of an incident but, instead, should work on getting the basics correct and maintain diligence, regardless of who you think is attacking and how they will attack. Speaking of attacks, do not underestimate the industry's adversaries. Cyberdefenders need to think like an attacker, not like a defender, and plan as if an attacker knows everything about your systems and network that you do—and is smarter. That might not be true, but it is the way to plan.

Perhaps most importantly, information and cybersecurity must be built into the design of every system. It needs to be built into every ship from the keel up, every application, every process and procedure. You must maintain an appropriate standard of care and follow industry best practices. And, most importantly, train and educate yourself, the technical staff, and your users—*people are the first line of defense*. Cybersecurity has to be an important part of the safety culture of which the maritime community is so justly proud.

Abbreviations and Acronyms

ABS	American Bureau of Shipping
AI	Artificial intelligence
AIS	Automatic Identification System
ALE	Annualized Loss Expectancy
APT	Advanced persistent threat
ARO	Annual Rate of Occurrence
ARPANET	Advanced Research Projects Agency Network
ATON	Aid to navigation
BAPLIE	Bayplan/Stowage Plan Occupied and Empty Locations message
BIMCO	Baltic and International Maritime Council
CAN	Controller Area Network
CCTV	Closed-circuit television
CEO	Chief Executive Officer
CERT/CC	CERT Coordination Center
CFR	U.S. Code of Federal Regulations
CGCYBER	U.S. Coast Guard Cyber Command
CIA	Central Intelligence Agency <i>or</i> Confidentiality, integrity, availability
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CODECO	Container Gate-In/Gate-Out Report message
COPRAR	Container Discharge/Loading Order message
COSCO	China Ocean Shipping Company
COTP	Captain of the Port
COVID-19	Coronavirus disease 2019
CPA	Closest Point-of-Approach alarm
CPS	Cyber-physical systems
DCS	Distributed control system
DDoS	Distributed denial-of-service attack
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	U.S. Department of Homeland Security
DoS	Denial-of-service attack
DOS	Disk Operating System
ECDIS	Electronic Chart Display and Information System
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport
EIA	Electronic Industries Alliance
ENISA	European Union Agency for Cybersecurity
EPIRB	Emergency Position Indicating Radio Beacon
EU	European Union
FBB	Fleet broadband
FBI	Federal Bureau of Investigation
ft	Feet
GB	Gigabytes (billions or 10 ⁹ bytes)
GFW	Global Fishing Watch
GLONASS	Global'naya Navigazionnaya Sputnikovaya Sistema
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GUI	Graphical user interface
HSMS	Hull stress monitoring system
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IACS	International Association of Classification Societies
IALA	International Association of Marine Aids to Navigation and Lighthouse Authorities
ICS	Industrial control systems
ICT	Information and communications technology
IDN	Integrated Digital Network
IEEE	Institute of Electrical and Electronics Engineers
IET	Institution of Engineering and Technology
IMO	International Maritime Organization

INS	Integrated Navigation System
IoS	Internet of Ships
IoT	Internet of Things
IP	Intellectual Property <i>or</i> Internet Protocol
IRNSS	Indian Regional Navigation Satellite System
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IT	Information technology
ITU-R	International Telecommunication Union, Radiocommunication sector
km	Kilometer
kn	Knots (nm/hour)
LAN	Local area network
LIDAR	Laser Imaging, Detection, And Ranging
LNG	Liquefied natural gas
LRIT	Long range identification and tracking
m	Meters
MARAD	Maritime Administration
MARSEC	Maritime Security program
MASS	Maritime Autonomous Surface Ships
MCS	Machinery Control Systems
MGO	Marine gasoil
MOB	Man overboard
MPA	Maritime and Port Authority
MSA	Maritime Safety Administration
MTS	Maritime Transportation System
MTSA	Maritime Transportation Security Act
M/V	Merchant vessel <i>or</i> Motor vessel
NATO	North Atlantic Treaty Organization
NavIC	Navigation with Indian Constellation
NAVTEX	Navigational telex
NGO	Non-governmental organization
NIST	National Institute of Standards and Technology
nm	Nautical miles
NMEA	National Marine Electronics Association
NSA	National Security Agency
OT	Operational technology
PHI	Protected health information
PII	Personally identifiable information
PIN	Personal identification number
PLC	Programmable logic controller
PNT	Positioning, navigation, and timing
POS	Point-of-sale
QA/QC	Quality analysis/quality control
QZSS	Quasi-Zenith Satellite System
RAT	Remote Access Trojan
RDP	Remote Desktop Protocol
ROI	Return on investment
SAE	Society of Automotive Engineers
SAR	Search and rescue
SART	SAR transponder
SATCOM	Satellite communications
SCADA	Supervisory Control and Data Acquisition
SIoT	Shipboard Internet of Things
SLE	Single Loss Expectancy
SMS	Safety Management Systems <i>or</i> Short Message Service
SOLAS	International Convention for the Safety of Life at Sea
SPI	Sensitive personal information
SQL	Structured Query Language
SSAS	Ship security alert system
SSL	Secure Sockets Layer

TB	Terabytes (trillions or 10^{12} bytes)
Tbps	Terabits (trillions or 10^{12} bits) per second
TEU	Twenty-foot equivalent unit
TSS	Transportation Systems Sector
UAV	Unmanned aerial vehicle
U.K.	United Kingdom
UN	United Nations
USB	Universal Serial Bus
US CERT	U.S. Computer Emergency Readiness Team
USCG	U.S. Coast Guard
UT	The University of Texas at Austin
UTC	Coordinated Universal Time
VDR	Voyage data recorder
VERMAS	Verified Gross Mass message
VHF	Very high frequency
VMS	Vessel monitoring system
VoIP	Voice over Internet Protocol
VPN	Virtual private network
VSAT	Very small aperture terminal
VTC	Vessel traffic control
VTS	Vessel Traffic Service
Wi-Fi™	IEEE 802.11 wireless LAN
Y2K	Year 2000

Acknowledgements

From Gary: Several people gave of their time and expertise to review this manuscript in fine detail, making content suggestions, and finding more typographical and grammar errors than I care to admit to (this sentence alone is giving them facial tics). I take full responsibility for any remaining errors or omissions. Thanks are due to:

- My wife and resident grammarian, Gayle M. Belin, M.A., CCC-SLP, Speech Language Pathologist
- My son and expert editor, Joshua R. Kessler
- Friend and colleague, Michael DeVold, Maritime Cybersecurity Manager, Royal Caribbean Cruise Lines
- Colleague and fellow Coast Guard Auxiliarist, Cliff Neve, CDR (Ret.), USCG and COO, MAD Security

Thanks also to Steve to helping me make this book a reality, and guiding this project through from start to finish and beyond.

From Steve: Two people agreed as well to learn far more about maritime cybersecurity than they ever wanted to, by serving as editors and sanity checkers.

- My wife, Sabine, who edits everything I write and is far better at this than she realizes;
- And, my son-in-law, Joe Plunkett, a professional cybersecurity analyst, not to mention great husband and father.

Thank you both. Again.

Figure and Table Credits

Figure 1.1. Screenshot from <https://shipfinder.co/>.

Figure 2.1. Public domain image, https://en.wikipedia.org/wiki/File:Wana_Decrypt0r_screenshot.png.

Figure 3.5. Screenshot from <https://www.marinetraffic.com/>.

Figure 3.6. Screenshot from <http://myship.com/>.

Figure 4.1. Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of Homeland Security.

Figure 4.3. International Trade Administration, U.S. Department of Commerce.

Figure 5.2. Screen shot from <https://www.shodan.io/>.

Figure 6.4. Captain Gurban Le Meur/Used with permission.

Figure 6.5. C4ADS/Used with permission.

Figure 6.6. SkyTruth/Used with permission.

Figure 6.7. *USNI News*/Used with permission.

Figure 7.3. IBM/Promare/Used with permission.

Figure 7.4. Kongsberg/Used with permission.

Figure 7.5. U.S. Coast Guard (USCG).

Figure 8.1. Chart by Gary C. Kessler, adapted from BIMCO/Used with permission.

Figure 8.2. Image used under license from ABSG Consulting Inc.

Figure 9.2. Original source unknown.

Table 2.1. National Institute of Standards and Technology (NIST), U.S. Department of Commerce.

Table 7.1. National Institute of Standards and Technology (NIST), U.S. Department of Commerce.

Table 8.1. U.S. Coast Guard Auxiliary.

All other figures and tables by the authors.

Gary C. Kessler



Gary C. Kessler, Ph.D., CISSP, is President of Gary Kessler Associates, a consulting, research, and training company located in Ormond Beach, Florida. He has been in the information security and education fields for more than 40 years, and is a retired professor of cybersecurity. Gary is a Principal Consultant at Fathom5, a Non-Resident Senior Fellow at the Atlantic Council, a visiting faculty member in the Electrical Engineering & Cyber Systems Section at the U.S. Coast Guard Academy, and has testified before the U.S. House of Representatives about maritime cybersecurity issues.

Gary has a B.A. in mathematics from Humboldt State College (California), an M.S. degree in computer science from the University of Vermont, and a Ph.D. in computing technology in education from Nova Southeastern University (Florida). His research interests focus on maritime cybersecurity, particularly related to AIS, as well as network protocols, digital forensics, and cybersecurity management and policy.

Gary is a member of the advisory board of the Maritime and Port Security Information Sharing and Analysis Organization (MPS-ISAO), Chief of the Cyber Augmentation Branch in the USCG Auxiliary, and a member of the USCG Research and Development Center (RDC) Auxiliary Support Unit. He is also a Master SCUBA Diver Trainer, holds a USCG master merchant mariner certificate, and holds a USCG Auxiliary coxswain qualification.

For more information, visit <https://www.garykessler.net> or contact Gary at gck@garykessler.net.

Steven D. Shepard



Dr. Steven Shepard is the founder of the Shepard Communications Group in Williston, Vermont, and co-founder of the Executive Crash Course Company. A professional author, photographer, audio producer, and educator with more than 35 years of experience in the technology industry, he has written books and articles on a wide variety of topics.

Steve received his undergraduate degree in Spanish and Romance Philology from the University of California at Berkeley, his master's degree in International Business from St. Mary's College, and his Ph.D. at the Da Vinci Institute in Rivonia, South Africa.

He is a Senior Fellow of the Da Vinci Institute of South Africa; a Founding Director of the African Telecoms Institute; and an Emeritus member of the Board of Trustees of Champlain College. He was Resident Director of the University of Southern California's Executive Leadership and Advanced Management Programs for more than 25 years and is adjunct professor at Emory University and the Da Vinci Institute, among others.

Thanks to a childhood spent in Spain, Steve is native fluent in Spanish and routinely publishes and delivers presentations in that language.

He lives in Vermont with his wife Sabine, who has put up with him for more than 45 years.

For more information, visit <https://www.ShepardComm.com>, or contact Steve at Steve@ShepardComm.com.

Index

- 3D printing , 171
- 5G , 162
- A**
- ABSG Consulting , 198
 - Active Directory (AD) , 83, 217
 - advanced persistent threat (APT) , 40, 41, 42, 74, 81, 101
 - aerospace , 98
 - AIDA Cruises , 85
 - aids to navigation (ATONs) , 19, 20, 21, 142
 - AIS SAR transponders (AIS-SART) , 141
 - AIS spoofing , 138, 144, 146, 148, 149, 150, 151, 152, 190, 192
 - AIS vulnerabilities , 142
 - all-hazards approach , 223
 - Amazon Web Services (AWS) , 51
 - American Bureau of Shipping (ABS) , 131, 198, 205
 - AmosConnect , 128
 - Android , 35, 50, 66
 - Annual Rate of Occurrence (ARO) , 188, 189, 213
 - Annualized Loss Expectancy (ALE) , 188, 189, 213
 - anti-malware , 212
 - Apache Software Foundation (ASF) , 50
 - APT29 , 101
 - Arabian Sea , 91
 - Arduino , 121
 - Argentina , 83, 151
 - ARPANET , 155
 - artificial intelligence , 91, 158, 161, 170, 172, 174
 - Asia , 82, 90, 98, 173, 182
 - AstraZeneca , 101
 - ATRIA , 145
 - ATT@CK Framework , 56, 57, 58
 - attack vectors , 165
 - Aurora Generator Test , 163
 - Austal , 77
 - Australia , 52, 76, 77, 84, 105
 - Australian Customs and Border Protection Service , 105
 - Australian National Lines (ANL) , 85
 - authentication , 32, 106, 117, 119, 123, 142, 164, 169, 211
 - authenticity , 32
 - Autoferry , 175
 - Auto-Maskin , 119, 168
 - Automatic Identification System (AIS) , 26, 86, 89, 115, 127, 132, 133, 139, 140, 141, 142, 143, 144, 152, 170, 171, 178, 190, 220
 - autonomous , 24, 172, 206
 - autonomous cargo , 182
 - autonomous cargo carrier , 173, 176, 177
 - autonomous commercial vessels, 172, 173, 178
 - autonomous devices , 156
 - autonomous maritime systems , 182
 - autonomous military vessels, 179
 - autonomous mooring , 177, 182
 - autonomous operations , 172
 - autonomous ships , 24, 181, 182, 196
 - autonomous systems , 155, 206
 - autonomous tug , 177, 181
 - autonomous UAVs , 182
 - autonomous vehicles , 157
 - autopilot , 134
 - availability , 32
 - aviation , ix, 16, 19, 84, 95, 98, 157
- B**
- Bab el-Mandeb Strait , 137
 - backdoor , 35, 75, 126, 129, 169
 - Bad Actor , 24, 25, 33, 39, 42, 46, 64, 66, 67, 74, 86, 88, 100, 121, 124, 126, 127, 142, 169, 171, 220
 - ballast , 26, 115, 118, 119, 120, 166
 - Baltic and International Maritime Council (BIMCO) , 131, 187, 194, 195
 - Bandar Abbas , 110
 - barge , 19
 - Bastø Fosen , 174
 - BASTØ FOSEN VI , 174

Battle of the Atlantic , 221
Bayplan/Stowage Plan Occupied and Empty Locations (BAPLIE) , 122
BeiDou , 135
Belgium , 105
Berthing Data , 171
big data , 170, 172
bills of lading , 100, 106
Bitcoin , 30, 35, 39, 44, 109
Black Hat , 126, 127
Black Sea , 145, 149, 150
Bluetooth , 65
board of directors , ix
Boeing 737 MAX 8 , 163
Bosporus Strait , 137
botnet , 38, 74, 124, 164
Brazil , 83
bridge systems , 117
broadband cellular , 162
brute force attack , 44, 47
brute force login , 107
Bureau Veritas Group (BVG) , 205, 206, 207
business e-mail compromise (BEC) , 44
BVG Guidance Note NI 641 , 206
BVG Rule NR 659 , 206

C

California Consumer Privacy Act (CCPA) , 215
cameras , 22, 48, 123, 124, 170, 178
Canada , 52, 79, 83, 90
Captain of the Port (COTP) , vii, xi, 112, 201
car carrier , 120
cargo , x, 20, 21, 22, 23, 24, 26, 81, 93, 95, 96, 98, 101, 105, 106, 114, 120, 140, 166, 170, 173, 182, 186
cargo handling , 22, 96, 116, 168, 196
cargo security , 23
cargo tracking , 22
Carnival Corp. , 77, 80, 84
Cellular at Sea , 114
Censys , 125, 164
Central Intelligence Agency (CIA) , 43, 81
centrifuges , 70, 160, 163
Channel 16 , 113
CHASITYBROOKE , 143
Chevron , 70
Chief Executive Officer (CEO) , ix
Chief Financial Officer (CFO) , ix
Chief Information Security Officer (CISO) , xi, 104
Chief Marketing Officer (CMO) , ix
Chief Operating Officer (COO) , ix
Chief Strategy Officer (CSO) , ix
Chile , 83
China , 41, 47, 72, 74, 79, 81, 89, 90, 91, 135, 147, 148, 151, 152, 180
China Ocean Shipping Company (COSCO) , 77, 83
China Overseas Port Holding Company , 91
Chinese People's Liberation Army Navy (PLAN) , 180
Chinese People's Liberation Army (PLA) , 41
CIA triad , 32, 34
circle spoofing , 147, 148, 152
class societies , 205
ClassNK , 205, 207
Clearance Time to Enter Port , 171
Clinton Administration , 204
closed-circuit television (CCTV) , 95, 115
closest point-of-approach (CPA) , 142, 145
CMA CGM , 85
CNC , 85
coastline , 20
CoinTicker , 35
COLREGS , 178, 220
Combat Command and Control Systems , 116
Common Vulnerability and Exposures (CVE) , 55
communication systems , 115, 125, 196
communications platforms , 128
communications technology , 95, 172
complacency , 43, 216
computer security , 31
confidentiality , 32, 44
container , 102, 103, 105, 106, 109, 120, 122, 123, 146, 168, 170, 173
Container Discharge/Loading Order (COPRAR) , 122
Container Gate-In/Gate-Out Report (CODECO) , 122
container ports , 90
containers , 170

Controller Area Network (CAN) , 134
 Cooperative Cognitive Maritime Cyber Physical System (CCMCPS) , 168
 copycat hardware , 44
 cost-benefit analysis , 213
 COVID-19 , 64, 84, 103, 104, 174, 175, 187
 Cozy Bear , 101
 CrashOverride , 163
 credential harvesting , 73
 credibility , ix, x
 crew , 23, 118, 125
 Crimea , 149, 150
 critical infrastructure , 135
 cryptocurrency , 35, 39, 44
 cryptojacking , 44
 Cyber Academy , 207
 Cyber Protection Team (CPT) , xi, 202
 Cyber Resilience Center , 104
 Cyber Resilience Review , 203
 cyber response team , vii, xi
 cyber risk , viii, 31, 197, 205, 213
 Cyber Security Evaluation Tool (CSET[®]) , 203
 Cyber Security Operations Center , 104
 Cyber Security Reporting Portal , 207
 cyberactivist , 52
 cyberattack , viii, 15, 21, 22, 33, 40, 41, 94, 96, 97, 101, 119, 159, 165
 cyberattack response , 204
 cyberattack tools , 53
 cyberattack vectors , 21, 24, 27, 33, 95, 119, 223
 cyberattacker , viii
 cyberattacks , 75
 cybercrime , 52
 cybercriminal , 29, 39, 52, 79, 83, 88, 105, 163, 172, 192
 cyberdefense , viii, 25, 41, 55, 111, 112, 131, 185, 193, 198, 211, 216
 cyberespionage , 95
 cyberfraud , 78
 cyberhygiene , 33, 117, 186, 211
 cyber-physical systems (CPS) , 96, 157, 159, 161, 162, 165, 172, 203
 cybersecurity , viii, x, xi, xii, 25, 27, 29, 30, 31, 33, 48, 49, 94, 104, 185, 203, 206, 216, 220
 Cybersecurity 101 , 211
 Cybersecurity and Infrastructure Security Agency (CISA) , 16, 106, 202, 203
 Cybersecurity Maturity Model Certification (CMMC) , 64
 cybersecurity maxim , 65, 217, 222
 cybersecurity planning , 193
 cyberspace , 31, 33, 109, 189, 201, 213, 216
 cyberspy , 53
 cyberstalker , 88
 cyberterrorist , 53
 cyberthreats , 27, 69, 104, 193, 196, 223
 cyberwar , 42, 53, 95, 110
 cyberwarrior , 53
 Cyprus , 79, 119, 146

D

D3FEND Framework , 56, 57
 daemon , 38
 Danaos Management Consultants , 85
 Dark Web , 54
 DarkComet , 74
 data alteration , 45
 data breach , 45, 187, 215
 data diddling , 45
 data leakage , 45
 data theft , 46
 database , 36, 45, 77, 98, 206
 De Hoop , 174
 Death Kitty , 109
 DEF CON , 119, 127
 Defense Federal Acquisition Regulation Supplement (DFARS) , 63, 64
 defense in depth , 212
 DEFIANT , 180
 denial-of-service (DoS) , 32, 38, 48, 95, 116, 142, 179
 Denmark , 177
 Designing the Future of Full Autonomous Ship (DFFAS) Project , 176
 digital ropes , 171
 digital twins , 171
 digitalization , 157, 158
 digitization , 157, 158
 disgruntled employees , 47
 Disk Operating System (DOS) , 130
 distributed control system (DCS) , 160, 161
 distributed denial-of-service (DDoS) , 38, 39, 124, 164

Djibouti , 90
DoD Advanced Research Projects Agency (DARPA) , 168
Domain Name System (DNS) , 48, 217
domains of war , 109
Doppelpaymer , 85
dredge , 21
Dridex , 74
drilling platforms , 21
drones , 24, 171, 177, 182
dynamic positioning system , 174

E

eavesdropping , 46, 47, 116, 121, 125, 127, 142
echo sounder , 134
e-commerce , 22, 26, 83, 100
Egypt , xiii, 102, 128, 146
Electronic Chart Display and Information System (ECDIS) , xi, 115, 118, 134, 186
Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) , 116, 122
Electronic Technical Manual , 167
ELISA LARUS , 207
e-mail fraud , 44
e-mail scams , 46
Emergency Position Indicating Radio Beacons (EPIRB) , 141
Emotet , 73
encryption , 113, 117, 119, 137, 164, 169
engine control systems , 118
ENRICA LEXIE , 124
Enterprise Mission Platform (EMP) , 201
Epsilon Algorithm Suite , 139
espionage , 42, 53, 89
EternalBlue , 43, 81, 82, 83
Ethereum , 44
Ethernet , 118, 134
Ethiopian Airlines Flight 302 , 163
Europe , 82, 98, 170, 173, 182, 198
European Union (EU) , 135, 146, 150, 215
European Union Agency For Cybersecurity (ENISA) , 111, 198, 199
Europol , 29
EVER GIVEN , xiii, 102
exploits , 220, 222
extortion , ix, 77
EXXON VALDEZ , 140

F

FALCO , 174
Federal Bureau of Investigation (FBI) , 36, 78, 106, 108, 111, 164
financial fraud , 36
financial management , 22
Finferries , 174
Finland , 174
FireEye , 101
firewall , 43, 186
fishing , 21, 114, 116, 123, 125, 140
fishing fleet spoofing , 151
fog of war , 54
France , 85, 90
FU XING 12 , 152
Fujian Mawei Shipbuilding , 79
Furuno , 124, 125, 177

G

Galapagos Islands , 151
Galileo , 135
gaming , 35
Garmin , 77, 84
Gelendzhik , 145
General Communications Headquarters (GCHQ) , 102
General Data Protection Regulation (GDPR) , 215
Germany , 30, 65, 66, 90
Ghana , 83
ghost ATONs , 143
Ghost Fleet Overlord , 180
ghost vessel , 190
Gibraltar , 146
Global Fishing Watch (GFW) , 151
Global Navigation Satellite Systems (GNSS) , 96, 115, 124, 132, 133, 134, 135, 137, 139, 141, 152, 170, 178, 217
Global Positioning System (GPS) , 24, 26, 125, 134, 135, 136, 137, 139, 152, 155, 186, 201
Globalstar , 114, 125, 126
GLONASS , 135, 137

GNSS interference , 145
GNSS spoofing , 138, 145, 146
GOLDEN RAY , 120
Google , 41, 165
GPS interference , 146
GPS jamming , 136, 137, 190
GPS spoofing , 137, 138, 139, 144, 146, 147, 148, 149, 152, 190
graphical user interface (GUI) , 130, 161
Greece , 85, 90
Gulf of Mexico , 70
Gulf of Tonkin Incident , 150
Gulf of Tonkin Resolution , 151
Gwadar Port , 91
gyroscope , 134

H

hackers , 75, 171
hacking , 41, 42, 46, 48, 52, 75, 81, 95, 111, 117, 179
hacking as a service , 55
hacktivist , 52, 192
Harry Potter , 29
healthcare , 162
high intensity radiated field (HIRF) , 127
HIKA , 152
HMS DEFENDER , 149, 150
HMS QUEEN ELIZABETH , 150
HNLMS EVERSTEN , 149
HOEGH OSAKA , 120
Holland , 90
Holland America Line , 80
Hong Kong , 90
host exploit , 46
Huangpu Maritime Safety Administration (MSA) , 147, 148
Huangpu River , 146, 147
hull stress monitoring system (HSMS) , 123
Hurtigruten , 85
Hypertext Markup Language (HTML) , 73, 126
Hypertext Transfer Protocol (HTTP) , 117
Hyundai Merchant Marine (HMM) , 74

I

IACS 166 , 206, 207, 208
IACS Requirement E22 , 206
IBM , 104, 174
ICS Joint Working Group (ICSJWG) , 203
identity theft , 36, 44, 52
IHS Markit , 185, 186
illegal, unreported, and unregulated (IUU) , 151
IMO 2021 , 131, 132, 197
India , 29, 70, 124, 135, 181
Indian Regional Navigation Satellite System (IRNSS) , 135
Indonesia , 70
industrial control systems (ICS) , 96, 120, 128, 159, 161, 169, 178, 194, 203, 207
industrial espionage , 89
industrial revolution , 158
Industry 4.0 , 158
ineffective disposal , 46
ineffective testing , 47
infected file , 34
information and communications technology (ICT) , 95, 113, 132, 159, 161, 167, 169, 178, 198, 199, 201, 218
Information Fusion Centre (IFC) , 105
information leakage , 86
information sharing , 200, 201, 203, 204, 205, 211
Information Sharing & Analysis Centers (ISACs) , 204
Information Sharing & Analysis Organizations (ISAOs) , 204
information technology (IT) , 104, 128, 164, 196, 199, 206
inland waterway system , 19
Inmarsat , 114, 128, 129
insider threat , 47
Institute of Electrical and Electronics Engineers (IEEE) , 139
Institution of Engineering and Technology (IET) , 112, 199
insurance , 40, 53, 78, 98, 187, 193, 197, 208
integrated digital network (IDN) , 155, 156
integrated navigation system (INS) , 133, 134, 141
integrity , 32
intellectual property (IP) , 41, 89, 91, 215
intellectual property theft , 18, 23, 36, 42, 53
Intellian Fleet Broadband (FBB) , 114, 115
intelligent mooring systems , 168
intermodal , 15, 16, 17, 19, 23, 93, 95

International Association of Classification Societies (IACS) , 131, 205
International Association of Ports and Harbors (IAPH) , 112, 199
International Chamber of Shipping , 194
International Convention for the Safety of Life at Sea (SOLAS) , 140, 196
International Electrotechnical Commission (IEC) , 183
International Maritime Cyber Centre of Excellence (IMCCE) , 207
International Maritime Organization (IMO) , 77, 89, 140, 146, 152, 196, 199
International Telecommunication Union, Radiocommunication Sector (ITU-R) , 139
International Union of Marine Insurance , 194
Internet , 22, 23, 26, 31, 34, 38, 40, 46, 48, 49, 54, 70, 77, 82, 86, 87, 100, 114, 115, 117, 119, 124, 125, 127, 128, 129, 131, 136, 137, 142, 155, 163, 170, 174, 214, 216, 217
Internet Explorer , 41
Internet of Ships (IoS) , 156, 167
Internet of Things (IoT) , 91, 156, 157, 161, 162, 163, 164, 165, 167, 168, 169, 170, 171, 172, 178, 182, 194
Internet Protocol (IP) , 107, 108, 123
intimidation , 36
intrusion detection , 186
inventory systems , 23
IoT cybersecurity , 162
Iran , 70, 75, 90, 109, 110, 121, 146, 148
Iridium , 114
IRIS LEADER , 176
Irish Sea , 150
Isle of Wight , 120
ISO 27001 , 104
Israel , 90, 91, 110, 146, 181
IT infrastructure , viii, 25, 26
IT organization , ix
Italy , 90, 124

J

Japan , 90, 121, 135, 175, 176, 177, 179, 207
JARI , 180
Jones Walker , 187
just-in-time , 103

K

Kawasaki Kisen Kaisha (K Line) , 77
Kazakhstan , 108
keystroke injection tool , 131
keystroke logger , 47, 74
keystrokes , 34
Kill Van Kull , 19
Kongsberg , 174

L

lack of input validation , 126, 128
LADY P , vii, viii, 212
large unmanned surface vessel (LUSV) , 180
laser imaging, detection, and ranging (LIDAR) , 178
law enforcement , 21, 40, 93
legal compliance , 22
Liberia , 108
Lightweight Directory Access Protocol (LDAP) , 51
Linux , 35, 50
liquefied natural gas (LNG) , 25, 207
Lloyd's of London , 53, 98, 205, 208
load balancing , 120
Log4j , 50, 51, 52
Log4Shell , 50, 51
logistics , 22
Long Range Identification and Tracking (LRIT) , 114, 115
low Earth orbit (LEO) , 139

M

machine learning , 172
Machinery Control Systems , 118
machine-to-machine (M2M) , 101, 161
MacOS , 35, 50
Maersk , 72, 76, 81, 83, 108, 217
MAERSK EINDHOVEN , 121
magnetic mines , 221
Mailto , 84
maintenance scheduling , 22
Malaysia , 78
malicious software (malware) , viii, ix, xi, 30, 32, 33, 34, 35, 37, 38, 39, 41, 42, 44, 45, 46, 47, 69, 70, 71, 73, 74, 76, 79, 90, 95, 98, 118, 134, 163, 165
malware , 188
man overboard (MOB) , 141

Maneuvering Characteristics Automation System (MCAS) , 163
 man-in-the-middle , 47, 116, 121, 179
 manipulation , 32, 33, 36, 95
 manufacturing , 17, 29, 98
 MANUKAI , 146, 147
 Marine Assets Corporation , 79
 Maritime & Port Security Information Sharing & Analysis Organization (MPS-ISAO) , 204
 Maritime Administration (MARAD) , 146
 Maritime and Port Authority (MPA) , 105
 Maritime Autonomous Surface Ships (MASS) , 196
 maritime cellular services , 114
 Maritime CEO Forum , 209
 Maritime Cyber Emergency Response Team (MCERT) , 207
 maritime cyber risk management , 188
 maritime cybersecurity , 188, 193, 208
 Maritime Cybersecurity Operations Centre (MSOC) , 105
 Maritime Information Sharing & Analysis Center (ISAC) , 204
 Maritime Modal Sector Coordinating Council (SCC) , 203
 maritime risk management , 188
 Maritime Safety Committee (MSC) , 197
 Maritime Security (MARSEC) , 104
 Maritime Security Council , 204
 Maritime Transportation Sector Information Sharing & Analysis Center (MTS-ISAC) , 205
 Maritime Transportation Security Act (MTSA) , 112, 202
 maritime transportation system (MTS) , xii, 15, 17, 20, 21, 25, 27, 88, 93, 96, 164, 167, 172, 185, 201, 223
 maritime waterways , 21
 marketing , ix, 22
 Masterly , 178
 MAYFLOWER , 174, 175
 Mayflower Autonomous Ship , 174
 meaconing , 138
 mechanical systems , 115
 Mediterranean Sea , 138, 145
 Mediterranean Shipping Company (MSC) , 76
 medium Earth orbit (MEO) , 135
 medium unmanned surface vessel (MUSV) , 180
 MEGURI 2040 , 175, 176
 merchant vessels , 16, 152
 message integrity , 142
 microprocessors , 155
 Microsoft , 41, 42, 70, 74, 77, 81, 82, 109, 130
 Microsoft Exchange , 74, 77
 Microsoft Outlook , 77
 MIKAGE , 177
 military , 21, 84, 93, 140, 170
 minesweeper , 220
 MIST , 123
 Mitre Corp. , 55, 57
 Mitsubishi Heavy Industries , 177
 Mitsui O.S.K. Lines (MOL) , 177
 mobile device , 34
 Mobile Maritime Service Identity (MMSI) , 140
 Monero , 39, 44
 Moore's Law , 155
 moorings , 21
 Morocco , 123
 MTS cyberdefense , 211
 MTS cybersecurity , 211
 MTS stakeholders , 201, 205
 music sharing , 35
 My Friend Cayla , 65

N

National Health Service , 29
 National Initiative for Cybersecurity Education (NICE) , 60
 National Institute of Standards and Technology (NIST) , 55, 58, 63, 64, 102, 183, 194
 National Maritime Cybersecurity Plan (NMCP) , xiii, 210
 National Security Agency (NSA) , 43, 57, 81
 National Vulnerability Database (NVD) , 55
 Nautilus Minerals , 79
 Naval Dome , 117
 Navigation and Vessel Inspection Circular (NVIC) , 112
 navigation rules , 178, 220
 navigation systems , 115, 133
 Navigation with Indian Constellation (NavIC) , 135
 Navigational telex (NAVTEX) , 134
 Navionics , 77
 NAVSTAR , 136
 NELLIE BLY , 177
 Nemty , 84
 Netherlands , 149, 170, 174

network security , 31
network segmentation , 186, 212
New Zealand , 52, 151
Newark Liberty Airport , 137
NICE Framework , 60, 61, 62
Nigerian 419 scams , 46
Nippon Foundation , 175
Nippon Kaiji Kyokai , 207
NIST Cybersecurity Framework , 58, 194, 202, 203
NMEA 0183 , 140
non-governmental organization (NGO) , 199, 205
North America , 98
North Atlantic Treaty Organization (NATO) , 91, 102, 149
North Korea , 30, 152
Norway , 84, 85, 174, 175, 178
Norwegian Maritime Authority , 174
Norwegian University of Science and Technology (NTNU) , 175
NotPetya , 82, 83
NYK Line , 176

O

O.MG cable , 44
Ocean of Things (OoT) , 168
OCEAN PEARL , 78
Office 365 , 76
open source , 40
open source intelligence (OSINT) , 46, 48, 86, 88, 89
Operation Aurora , 41, 42
operational technology (OT) , viii, 96, 104, 111, 132, 155, 158, 159, 163, 164, 165, 166, 167, 168, 170, 171, 172, 173, 178, 182, 186, 196, 198, 199, 201, 203, 206, 218
Operational Technology Information Sharing & Analysis Center (OT-ISAC) , 205
Orca AI , 176
Orion , 101
OT cybersecurity , 166
Oxford University , 128

P

packet switching , 155
Pakistan , 91
Panama , 83, 207
Panama Canal , 19, 137, 180
Panama Maritime Authority , 207
Panix , 38
paperless navigation , xi
Parkerian Hexad , 32, 190
passengers , x, 16, 20, 21, 23, 95, 96, 129, 140, 215
password cracking , 44
password spraying , 47
patches , 42, 50, 132, 212
payroll , 22, 23, 107
Pen Test Partners , 66, 122, 123
people-to-machine (P2M) , 161
performance , 34
personal identification number (PIN) , 106, 169
personally identifiable information (PII) , 18, 35, 84, 85, 109, 215
personnel management , 22, 23
Peru , 83
phishing , 32, 35, 36, 37, 41, 48, 72, 78, 80, 95, 107, 108, 188
physical exploit , 48
physical security , 22, 104, 204
pilot boats , 96
pirates , 75
PNT augmentation , 139
PNT Integrity Library , 139
Point Reyes , 148
point-of-sale (POS) , 47, 116, 129
Poland , 71
policies and procedures , 162, 185, 193, 196, 212
Ponce de Leon Inlet , 143
pornography , 35, 71, 131
port , vii, viii, ix, x, 18, 20, 22, 23, 24, 26, 93, 94, 95, 96, 97, 98, 100, 101, 104, 107, 122, 171, 215
port authority administration , 95
port cybersecurity , 93, 105, 198
Port de Barcelona , 108
Port of Antwerp , 105
Port of Brunswick , 121
Port of Cape Town , 109
Port of Dakhla , 123
Port of Durban , 109
Port of Houston , 106

Port of Kalama , 108
Port of Kennewick , 109
Port of Long Beach , xiii, 20, 83, 103
Port of Longview , 108
Port of Los Angeles , xiii, 20, 83, 103, 104
Port of New York and New Jersey , x, 212
Port of Novorossiysk , 145
Port of Rotterdam , 170
Port of San Diego , 109
Port of Shanghai , 146, 148
port stakeholders , 104, 169, 199
port tenants , 22
PortDoor , 81
ports , 15
position, navigation, and timing (PNT) , 24, 96, 133, 136, 139, 152, 178
possession , 32
power , 21, 26, 116, 140
power grid , 136, 159, 163
PRABHU DAYA , 125
Precise Positioning Service (PPS) , 136
Princess Cruises , 80
programmable logic controller (PLC) , 160, 161, 163
Promare , 174
propulsion , 26, 118, 161, 166, 186, 196
protected health information (PHI) , 35, 81, 215
public safety , 21, 170

Q

qualitative risk assessment , 189
quantitative risk assessment , 188, 213
Quasi-Zenith Satellite System (QZSS) , 135

R

radar , 118, 124, 134
Ragnar Locker , 85
railroad , ix, 16, 19, 95, 101
ransomware , ix, 29, 30, 32, 39, 40, 43, 52, 81, 82, 83, 84, 95, 108, 109, 188
ransomware as a service , 55
Raspberry Pi , 121
reconnaissance , 48, 111
Red Funnel , 76
regulatory , ix, 97, 113, 114, 131, 187, 200, 202
Remote Access Trojan (RAT) , 35, 74
Remote Desktop Protocol (RDP) , 109
reservation systems , 22
resilience , 217
resource exhaustion , 38
retail , 98, 100, 162
return on investment (ROI) , 213, 216
return on negligence (RON) , 214
risk analysis , 188
risk assessment , 188, 192
risk assessment model , 195
risk management , 213
robocalls , 37
Rolls-Royce , 174
route management , 22
Royal Caribbean , 174
Russia , 29, 81, 90, 101, 108, 111, 135, 145, 147, 148, 149, 150, 174, 181

S

Safer Vessel with Autonomous Navigation (SVAN) , 174
Safety at Sea , 187
Safety Management Systems (SMS) , 131
salami attack , 48
sales , 22, 23, 100
SamSam , 109
satellite , 114, 117, 118, 125, 126, 128, 136
satellite communications (satcom) , 125, 126
Saudi Arabia , 146
SCUBA , 67
SEA FOX , 143
SEA HUNTER , 179
Sea Machines , 177, 180
search and rescue (SAR) , 141, 142, 181
security credentials , 25
sensitive personal information (SPI) , 215
sensors , 22, 115, 119, 123, 134, 155, 157, 160, 161, 164, 167, 168, 169, 170, 171
Server Message Block (SMB) , 82

session hijacking , 49, 127
 Shahid Kaveh , 120
 Shahid Rajaei Port , 110, 121
 Shen attack , 98
 Shin Nihonkai Ferry Co. , 177
 ship , 113, 124, 130, 146, 168, 174, 206
 ship monitoring and security systems , 115
 Ship Security Alert System (SSAS) , 115
 Shipboard Internet of Things (SIoT) , 156, 167
 shipboard networks , 117, 129
 shipboard security systems , 123
 shipping lines , x, 15, 22, 23, 25, 77, 100, 204, 208, 215
 Shodan , 125, 126, 164
 Siemens , 70, 160, 163
 SIGINT , 151
 SILVER ORIGIN , 174
 Silversea Cruises , 174
 Singapore , 79, 105, 125, 181, 207
 Single Loss Expectancy (SLE) , 188, 189, 213
 smart grid , 157
 smart ports , 162, 169, 170, 171
 smart ships , 162, 167, 170, 207
 smishing , 37
 Sochi , 145
 social engineering , 32, 33, 35, 37, 41, 48, 80, 106, 107
 social media , 88, 89, 123
 Society of Automotive Engineers (SAE) , 172
 Sodinokibi , 84
 Software vulnerability databases , 55
 SolarWinds , 101, 102
 SOLEIL , 176
 sonar , 134
 South Africa , 109
 South Korea , 69, 90
 Spain , 30, 90, 108
 spearphishing , 36, 37, 73, 81, 90, 108, 111
 spies , 47
 spoofing , 137, 138, 139, 144, 145, 146, 147, 148, 149, 152, 190, 192
 spyware , 34, 78
 SQL inject , 128
 Sri Lanka , 90
 St. Petersburg , 145
 Standard Positioning Service (SPS) , 136
 StarLink , 114
 status monitoring , 26
 Steamship Authority (SSA) , 85
 STENA IMPERO , 146
 Step7 software , 70, 163
 Strait of Gibraltar , 137
 Strait of Hormuz , 110, 137, 146
 Strait of Malacca , 137
 strategy , 97, 185, 211
 Stuxnet , 70, 160, 163, 198
 STX3 chip , 125
 Suez Canal , xiii, 19, 102, 137
 SUNBURST , 101
 SUPERNOVA , 102
 Supervisory Control and Data Acquisition (SCADA) , 161
 supply chain , xiii, 18, 49, 98, 99, 103, 162
 supply chain management , 23
 supply management , 22
 survey , 185, 186, 187
 SUZUKA EXPRESS , 87
 Svitzer , 76
 Sweden , 119
 Switzerland , 76
 SW-Registry , 206
 Syria , 119
 SYS-COM , 206

T

Taiwan , 29
 Tallinn Manual , 110
 telecommunications , viii
 Telnet , 117
 Templar Executives , 207
 terminal , 94, 95
 Terminal Operating System (TOS) , 109
 TEUs , 106
 The Shadow Brokers , 81
 The Solent , 120

threats , 220, 222
thumb drive , 33, 70, 118, 130, 131, 134
Tidal Window , 171
timestamp , 142
timing signal , 135
TITANIC , 196
Togo , 78
Toll Group , 84
training , 107, 171, 178, 186, 193, 200, 202, 204, 205, 207, 212, 218, 219
transistor , 155
Transnet , 109
transportation , x, 20, 98, 159, 162
Transportation Systems Sector (TSS) , 16, 203
trickery , 36
trilateration , 135
Trisis , 163
Triton , 163
Trojan horse , 24, 34, 35, 66, 73, 74
trucking , ix, 16, 19
trust , ix, 37
tugs , 24, 96
Tunisia , 128
Turkey , 181

U

U.S. Air Force , 136
U.S. Coast Guard (USCG) , xi, 104, 112, 144, 146, 180, 194, 200, 201, 202, 212
U.S. Coast Guard Academy , 202
U.S. Coast Guard Cyber Command (CGCYBER) , 106, 200
U.S. Computer Emergency Readiness Team (US-CERT) , 203
U.S. Defense Logistics Agency (DLA) , 78
U.S. Department of Defense (DoD) , 63, 64, 168, 200, 201
U.S. Department of Energy (DOE) , 194
U.S. Department of Homeland Security (DHS) , 55, 101, 111, 139, 162, 200, 202
U.S. Department of Justice , 109
U.S. Navy , 88, 90, 136, 151, 179, 180
U.S. Space Force , 136
Ukraine , 29, 83, 149, 150
unauthorized access , 50
United Arab Emirates (U.A.E.) , 79, 91, 181
United Kingdom (U.K.) , 29, 52, 76, 82, 90, 120, 146, 149, 150, 174, 199
United Nations (UN) , 122, 196, 199
United States (U.S.) , x, 20, 40, 47, 52, 63, 78, 79, 83, 85, 90, 101, 103, 106, 107, 108, 109, 110, 111, 120, 135, 140, 143, 148, 150, 151, 174, 177, 179, 180, 187, 200, 203, 215
United States Code of Federal Regulations (CFR) , 141
Universal Serial Bus (USB) , 44, 70, 96, 118, 130, 131, 134
University of Texas at Austin , 138
unmanned , 24
unmanned aerial vehicle (UAV) , 182
unmanned surface vessel (USV) , 179, 181
unpatched systems , 50
Uruguay , 83
USB Rubber Ducky , 131
USCG Research and Development Center (RDC) , 180
users , 218
USS KIDD , 88
USS MADDIX , 150
USS ROSS , 150
USS TICONDEROGA , 150
USS TURNER JOY , 150
utility , 32

V

Vard Group , 84
Verified Gross Mass (VERMAS) , 122
very high frequency (VHF) , 113, 115, 124, 139, 142
very small aperture terminal (VSAT) , 114, 115, 127
vessel identity laundering , 151
vessel monitoring systems (VMS) , 114, 116
vessel tracking , 86, 89
vessel traffic control (VTC) , 24, 26
vessel traffic management , 22, 96, 141
Vessel Traffic Service (VTS) , vii
Vietnam , 150, 151
virtual private networks , 26, 114
virtual reality , 171
virus , 34, 39
vishing , 37
Vladivostok , 145
Voice over Internet Protocol (VoIP) , 114, 127

voicemail , 108
voyage data recorder (VDR) , 118, 123, 124, 186
vulnerabilities, 32, 126, 220, 222

W

WannaCry , 30, 34, 39, 43, 82, 83, 217
Wärtsilä , 207
watering hole attack , 35, 37, 111
website , 26
whaling , 36
whistleblowers , 47
WHITE ROSE OF DRACHS , 138
Wi-Fi , 96, 129, 155, 170
WikiLeaks , 43, 81
wind turbines , 21
Windows , 35, 50, 70, 73, 74, 82, 83, 130, 131, 134, 160
Windows 7 , 50
Windows XP , 50, 82
work boats , 21
World Fuel Services (WFS) , 78
World Shipping Council , 194
worm , 34, 39, 70

Y

Y2K , 214
Yangtze River , 148
YARA BIRKELAND , 177, 182
YUK TUNG , 152

Z

ZENOBIA , 119
Zero Trust , 62, 63, 212
zero-day exploits, 42, 43, 70, 74, 106, 218
ZIM GENEVOA , 117
Zoho ManageEngine , 106
zombie , 38
zombie network , 34

[1] With apologies to Sir Edward George, Earle Bulwer-Lytton and Snoopy.

[2] Adapted from Cook & Nichols, 2017.

[3] <https://cve.mitre.org/>

[4] <https://nvd.nist.gov/>

[5] <https://attack.mitre.org/>

[6] <https://d3fend.mitre.org/>

[7] <https://www.nist.gov/cyberframework>

[8] Once hackers break into a system, they often create a backdoor so that they can continue to access the compromised computer without having to “break in” to the system again. A common backdoor is to create a new user account with a high privilege level. They then remove the traces of their attack and log in in via the new account.

[9] The SMB service provides file, printer, device, and other forms of resource sharing on Windows networks.

[10] The so-called *kill switch* was an Internet domain name. The WannaCry code looked for a particular domain and, if absent, continued to propagate. Once the domain name was registered, the attack stopped.

[11] Irregular size cargo that might or might not be containerized.

[12] A more complete list of vessel tracking sites can be found on the book’s associated Web page.

[13] Widely credited to former USCG Commandant ADM James Loy (ret.).

[14] There are, in general, three ways to authenticate one’s identity, namely by what you know (e.g., a password or a PIN), what you have (e.g., a TWIC or other identification), and what you are (e.g., a fingerprint or voiceprint). Authentication using just one of these mechanisms is called *single-factor authentication*. *Multi-factor authentication*, using at least two different mechanisms, is significantly stronger than single-factor authentication.

[15] The Tallinn Manual is a research initiative of the NATO Cooperative Cyber Defence Centre Of Excellence (CCDCOE). See <https://ccdcOE.org/research/tallinn-manual/>

[16] The reference list on the book’s website points to several papers with more detailed information about shipboard communications protocols.

[17] Telnet is a protocol that allows a user to remotely log in to a computer across the local network or Internet. Although Telnet access usually requires use of a password, it does not employ encryption.

[18] ZENOBIA is reputed to be one of the top 10 wreck dives in the world.

[19] EDIFACT provides a standard format so that different computer systems using different internal formats and data structures can exchange information.

[20] A *collision* occurs when two moving vessels strike each other, while an *allision* occurs when a moving vessel strikes a stationary object, such as a vessel made fast, a dock, or a bridge abutment.

[21] The industrial revolution started in the late-1700s with the introduction of mechanical processes, and the use of water and steam-powered engines in the mass production of goods. What is now called Industry 2.0 began in the early 20th century with the use of electrical energy to run machines and the introduction of the assembly line. Advances in computer and communications technology starting in the 1960s brought on Industry 3.0. Cyber-physical systems are the hallmark of Industry 4.0.

[22] “No man will be a sailor who has contrivance enough to get himself into a jail; for being in a ship is being in a jail, with the chance of being drowned ... a man in a jail has more room, better food, and commonly better company.” Samuel Johnson (1709-1784)

[23] The inclusion or exclusion of an organization or document is not to be construed as a recommendation, judgement, or reference. The order in which this information is provided has no significance.

[24] <https://www.nist.gov>

[25] <https://www.bimco.org>

[26] <https://www.imo.org>

[27] <https://ww2.eagle.org>

[28] <https://www.enisa.europa.eu>

[29] <https://www.theiet.org>

[30] <https://www.iaphworldports.org/>

[31] <https://www.uscg.mil>

[32] <https://www.cisa.gov>

[33] <https://us-cert.cisa.gov>

[34] <https://maritimesecurity.org>

[35] <https://mpsisao.org>

[36] <https://www.mtsisac.org>

[37] <https://www.otisac.org>

[38] <https://group.bureauveritas.com>

[39] <https://www.classnk.com>

[40] Louis Pasteur (1822-1895).

[41] There are many who will point out that using a two-digit year was due to limits of computer memory and other system constraints. While that might have been true in the 1960s and before, it does not explain why some of those programming practices extended into the 1980s and beyond. Author Kessler proudly observes that he has been writing Y2K-compliant code since 1973.

[42] John Donne (1752-1631)

[43] Credit to Scott O. Bradner, former University Technology Security Officer at Harvard University.

[44] A paraphrase of a quote originally about cryptography.

[45] Many variants attributed to many people but the sentiment seems to have originated with Helmuth von Moltke (1800-1091).

[46] A vulnerability in the Secure Sockets Layer/Transaction Layer Security (SSL/TLS) was reported in 2015. Dubbed the “Bar Mitzvah attack,” the vulnerability had been present in the protocol since 2002. More recently, the Log4j vulnerability had been present for eight years prior to being identified and exploited.