Hack@Sea

Paper

Paper Title: **Cyber Threats That the Maritime Industry Currently Face Around the Globe**

Made by:

Christopher Sulistiyo (4850025)

Supervised by:

Rob Loves

Jeroen Pijpker

Sietse Dijkstra

Stephen McCombie

Version Management

Version Number	Date	Remarks
1.0	08-12-2022	Initial peer review draft

Acknowledgement

The researcher would like to thank the following people for their contribution to the research and preparation to this paper in the form of remarks, feedback, and suggestion:

Rob Loves, Jeroen Pijpker, Sietse Dijkstra, and Stephen McCombie for their endless unwavering support, extensive resources, unlimited love and for never stop believing in the researcher.

Abstract

The MTS is a highly connected network of systems. When one system is compromised, it can affect other sub-systems, or the system as whole. Entering towards the digitalization era, MTS is increasingly reliant on information communication technologies on their automation sector when it comes to transportation, and that will continue to be so in the future especially with the development of fully automated ships. The MTS ecosystem consists of six interconnected systems, described in the following: ships, shipping lines, people, ports, intermodal transfers, and inland waters. Each of these domains can be further divided into several sub-domains, and all every aspect in the MTS 6 domains have ICT involved in them. In MTS, there are many kinds of ships that are currently traversed the oceans around the globe. The overwhelming majority of ships, excluding military vessels and yachts, can be divided into several broad categories: cargo carriers, passenger carriers, industrial ships, service vessels, and miscellaneous non-commercial vessels. Each category can be then subdivided, with the first category containing by far the greatest number of subdivisions. The cargo categories that ship carry can also be further divided into three categories, which are liquid, dry, and specialized cargoes. Ships can also be sub-categorized into several types of sails they use, the thickness of the mast, number of crews, number of decks, strength, weaknesses, utilities, and many more. Throughout the history, distinct kinds of regions with their vast difference of climate, along with different historical era progression each created unique ships that will require many pages scribble down.

A ship normally has different systems that are interconnected into one constitution for it to sail on the open water. These systems include the ship network, navigation, updates and remote access, communication system, crew network, the backbone of the network, industrial control systems, and loading and stability system of the ship. Moreover, while operating above the ocean, ships will make communication to ports very often. Ports are the microcosm of the entire MTS; they are the interface between ships and the land. While all ports around the globe differ in the details, they are similar at an exceedingly prominent level. Just like ships, a port consists of different components, myriad functions, agency, organizations, and people at port. Components of a port can be described as the following: the terminal gate functions as the secure entry point and is a component of the physical perimeter of the port, the terminal represents all information and communication technology systems at the port, terminal headquarters who hold data in an ICT system, industrial control systems and operational technology represent the cyber-physical systems at ports and on ships, and the Position, Navigation, and Timing system used for navigation and port logistic. Ships and ports all have many different and crucial components to the MTS that are interconnected to one another, and the essence of the cybersecurity challenge is to protect them from cyberthreats and attacks on information.

There are various kinds of attacks on the MTS that can be divided based on their technical approach and motivations. Such motivations include greed or theft of money, cargo, information, or simply the disruption of the system. Common cyber-attacks on the MTS throughout the history can be described as the following: ransomware, phishing attack, ghost shipping cyber-attack, and AIS and GNSS spoofing and jamming. All these attacks can be simplified into two diverse kinds of attacks, which are an attack on shipping company's business logistics systems, and an attack on ship's navigation systems (AIS and GNSS spoofing and jamming). It is also important to note that piracy is still happening in the maritime field and is still considered a threat to the MTS, although their cases are not as high as the cyber-attack. Furthermore, all these cyber-attacks can be realized and conceived of when looking at the common vulnerabilities that ships share to one another. The common cyber vulnerabilities, which may be found onboard existing ships, and on some newbuild ships, are included in the following: staff inadequately trained and/or skilled to manage cyber risks, missing and untested contingency plans and procedure, obsolete and unsupported operating systems, unpatched system software, outdated or missing antivirus software and protection from malware, safety critical equipment or systems always connected with the shore side, lack of boundary protection measures and segmentation of the shipboard computer networks, and inadequate access controls to cyber assets and networks for third party including contractors and service providers.

Table of Contents

Introduction

Background

CISA (Cybersecurity and Infrastructure Security Agency) and the DHS (Department of Homeland Security) have identified 16 critical infrastructure sectors whose assets, systems, and networks whether physical or virtual are considered so vital to the United States of America, the greatest country on Earth (*Donald J. Trump, 2016*) that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health, safety, or combination thereof (*see Figure 11 in the Appendix)* to the proud nation of United States of America, thus crippling other insignificant inferior countries by their economic sector as well.

Maritime is a part of transportation system that is identified as one of the most important infrastructure asset and is required by national policy (*see Homeland Security Presidential Directive 7*) to be strengthened and maintained by the supreme United States of America's government, as it is often subjected to potential lunatic terrorist attacks, as America's brilliantly open and technologically superior complex society includes a wide array of critical infrastructure that often attracts diabolical imbecile terrorist who seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the sovereign United States of America national security, cause mass casualties, weaken the economy, and damage public morale and confidence of the great nation of United States of America. Included in one of those attacks is the cyber-attack by the misbegotten and degenerate cyber-criminals around the globe.

One of sixteen sectors that will be subject of interest in this paper is the Transportation System Sector. And that specific sector itself consists of seven key sub-sectors, including aviation, highway and motor carrier pipeline, freight rail (trains), pipeline systems, mass transit and passenger rail, postal and shipping, and **maritime transportation system** (CISA, 2020). Maritime Transportation System itself consists about 95.000 miles of coastline, 361 ports, more than 25.000 miles of waterways, and intermodal landside connections that allow the various modes of transportation to move people and goods to, from, and on the water.

Maritime is shaped by the physical, geographical, political, and demographic characteristics of the planet Earth (*see Figure 1, 2, 3, and 4 in the Appendix*).

Maritime is a part of transportation system that is identified as one of the most important infrastructure asset and is required by national policy (*see Homeland Security Presidential Directive 7*) to be strengthened and maintained by the proud United States of America's government, as it is often subjected to potential terrorist attacks, as America's open and technologically superior complex society includes a wide array of critical infrastructure that often attracts terrorist who seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States of America national security, cause mass casualties, weaken the economy, and damage public morale and confidence of the great nation of United States of America. Included in one of those attacks is the cyber-attack by the cyber-criminals around the globe.

Cybercrime is a rapidly growing threat to all aspects of life, and the shipping and offshore industry are no exception. In the time of 1800s to early 1900s, all the aircraft flight- and maritime domain deck used analogue dials as the means of. Prior to the digitization era, safety of the ship was determined by. Digitization and connectivity introduce new opportunities. However, they also introduce unknown risk.

As of until now, maritime cyber-attacks are happening more frequently than members of the maritime community could believe because of the number of unreported and undetected attacks (Hayes, 2016). It is a real threat to the maritime industry, as increased security breaches are being reported. The safety of vessel is constantly at risk. Companies are losing millions of dollars. Crews, passengers, and environments are being put in danger. Those above statements are further strengthened by a statement from one of the admirals of United States Navy service branch: “We are vulnerable in the military and in our governments, but we are most vulnerable to cyber-attacks commercially. This challenge is going to significantly increase. It is not going to go away” - (Admiral Michael Mullen, USN). With that being said, the technologies that are currently used around the world are still looking forward to being even more modernized and further developed. Even now, there are companies which are conducting extensive research on having fully automated (AI-powered) ships, which means that there is no human being on the ship, and everything will be run through computerization. It means that the operating system of the ship can make decisions and determined actions by itself requiring no on-board members. The creation of fully autonomous ships brings new possibilities, but it also comes with an increased threat to cybersecurity. There is an old saying in the cybersecurity world that no computing device is inherently secure. If a device has a set of system hardware and software IT resources, it will automatically be at risk as there always be some ways for a hacker to exploit it and make use of it for their own benefits.

With those above statements being declared, it is particularly important to whoever work at the maritime industry to start realizing how important it is to learn cybersecurity as well as ways to mitigate the risk.

Research Reason

The worlds of maritime industry and cyber security are vast with both dependent on technology more than they were ever before. Although the maritime industry is a broad subject with many different skills and knowledge to be acquired depending on what position one is currently in at in its hierarchy level, the cyber security world is even broader with many different domains that is include but not limited to the IT domains of security (*see Figure 9 in the Appendix*). Each of these domains include separate roles, responsibilities, tools, technologies, processes, and many more that represents a piece of cyber security. When learning about the maritime cyber-security sector, one must be acknowledged of all the knowledge that maritime industry has to offer, albeit not all the cyber security competencies need to be taken into consideration, as it would make maritime cybersecurity an extremely complex topic. When learning about cyber-security, it is crucial for one to think like an attacker, not just as a defender, and plan as if an attacker knows everything about the systems and network that he/ she is planning to attack. Therefore, this paper will provide information about the basic knowledge to start when talking about cyber-attacks and potential cyber-threats that the maritime world is currently facing.

Research Goal

This research is conducted in the hope that the readers will gain an ample apprehension on what the Maritime Transportation System is, what are its crucial components and, how do ships operate in open water. Furthermore, after gaining the basic comprehension of the topics mentioned above, this paper will take readers further to what kinds of infamous cyber-attacks that have happened in the maritime industry, along with cyber vulnerabilities that the Maritime Transportation System still share and to what they could potentially lead. This paper aims to make a summary of all available sources and put it into a single intelligible research paper.

Additionally, this paper serves as half part of the grading criteria from the minor Hack@Sea of the NHL Stenden University of Applied Sciences, Emmen location, the Netherlands.

Reading Guide

Because of the intended purpose of the paper is to explain the introductory knowledge to the general audience, no mandatory reading is necessary prior to reading about this paper.

Definition of Terms

- OEM (Original Equipment Manufacturer): a company that manufactures products that are used as inputs to the production of another more complex product (Investopedia, October 29, 2021).
- IMO (International Maritime Organization): a specialised agency of the United Nations responsible for regulating shipping (Wikipedia, n.d.).
- OCIMF (Oil Company International Marine Forum): a voluntary association of oil companies having an interest in the shipment of crude oil, oil products, petrochemical and gas, and includes companies engaged in offshore marine operations supporting oil and gas exploration, development, and production (Wikipedia, n.d.)
- ISM (International Safety Management): the IMO standard for the safe management and operation of ships at sea (Wikipedia, n.d.)
- BIMCO (Baltic and International Maritime Council): one of the world's largest direct-membership organization for shipowners, charterers, shipbrokers, and agents (Wikipedia, n.d.).
- CISA (Cybersecurity and Infrastructure Security Agency): is an agency of the United States DHS that is responsible for strengthening cyber security and infrastructure protection across all levels of government, coordinating cyber security programs with U.S. states, and improving the government's cybersecurity protections against private and nation-state hackers (Wikipedia, n.d.).
- DHS (Department of Homeland Security): is the United States federal executive department responsible for public security, comparable to the interior or home ministries of other countries (Wikipedia, n.d.).
- VTS (Vessel Traffic Service): a marine traffic monitoring system established by harbour or port authorities, like traffic control for aircraft (Wikipedia, n.d.).
- AIS (Automatic Identification System): an automated, autonomous tracking system which is extensively use in the maritime world for exchange of navigational information between AIS-equipped terminals (MarineTraffic, n.d.).
- Gyrocompass: a type of non-magnetic compass which is based on fast-spinning disc and the rotation of the Earth to find geographical direction automatically (Wikipedia, n.d.).
- ICS (Industrial Control Systems): an area consisting of control components (e.g., electrical mechanical, hydraulic, pneumatic) that act together to achieve industrial objective, e.g., manufacturing, transportation of matter or energy (NIST, n.d.).
- GNSS (Global Navigation Satellite Systems): a general term describing a satellite constellation that provides position, navigation, and timing services on global or regional basis (NcYTE Centre, January 7, 2021).
- GPS (Global Positioning System): part of the GNSS constellation of international satellite systems that orbit the earth in which is owned by the country United States of America (NCyTE Centre, February 8, 2021).
- CCTV (Close Circuit Television): a video camera used to transmit a signal to a specific place, on a limited set of monitors (Wikipedia, n.d.).
- Cyber Resilience: ability to indicate the robustness of one information technology or operational systems (DNV Maritime, March 27, 2020).
- OT (Operational Technology): a hardware or software that detects, and causes a change, through the direct monitoring and/or control of physical devices such as industrial equipment, assets, processes, and events (Wikipedia, n.d.).
- ICT (Information and Communications Technology): an extensional term for IT that stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals) and computers, as well as necessary enterprise software, middleware, storage, and audio-visual, which enable users to access, store, transmit, understand, and manipulate information (Wikipedia, n.d.).

- Middleware/ “software glue”: type of computer software that provides services to software applications beyond those available from the operating system (IBM, March 21, 2021).
- IT (Information Technology): the use of computers, infrastructure, and components that enable modern computing such as to create, process, store, retrieve, and exchange all kinds of data and information (Wikipedia, n.d.).
- Malware (malicious software): any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private unauthorized access to information or systems, or which unknowingly interferes with the user’s computer security and privacy (Wikipedia, n.d.)
- Ransomware: a type of malware crypto virology that threatens to publish victim’s personal data or permanently block/ delete access to it unless a ransom is paid off (Wikipedia, n.d.).
- Phishing: a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message to trick a person into revealing sensitive information to the attacker or to deploy malicious software on victim’s infrastructure like ransomware (Wikipedia, n.d.).
- Social engineering: in the context of security, is the psychological manipulation of people into performing actions or divulging confidential information (Wikipedia, n.d.).
- AIS or GNSS spoofing: a type of cyber-attack where an authorized user sends false signals to an AIS or GNSS receiver to trick it into believing that it is located somewhere else (Whichsatnav, November 7, 2022).

Methodology

Instruments

During this research only qualitative data was collected, as all the research questions are answered through the needed data by the means of desk research. However, it is possible that each of the research question's answers may be expanded upon if needed or requested by the above-mentioned minor supervisors, as the content of the paper is limited, and the research answers are purposely condensed.

Population and Samples

The research samples were selected based on their purpose and convenience. Multiple articles online, and books through the form of electric or physical have been used regarding the research as well as sampling.

The population in this paper will be overly broad, from 9-12 graders to community college students to first- and second-year university students who are interested in the topic of cybersecurity in maritime industry. This paper will require little to no technical knowledge to understand the contents presented.

Limitations

Research question #1 shall answer all diverse types of ships that are currently operating around the globe. However, inscribing all the known ship types including ships that have made their mark in maritime history (such as the Schooner, the Brig, the Brigantine, the Carrack, etc.), will exceed the paper's limitation on its contents. Thus, the paper will only include the famously known ship types that are cited in various references and who are represented in the International Maritime Organization definition of ship conventions. Furthermore, research question #3 will discuss some of the cyber attack vectors of the Maritime Transportation System. The actual cyber-attack vectors around the globe are listed, but not limited to, in the answer to the above-mentioned research question.

The answers to all the research questions are the result of conflating the contents of multiple articles discussing the research subject online, due of the nature of the paper, which is purely based on desk research, the researcher therefore cannot sustain the reliability of the content except from the validity that the articles already presented to the audience.

Data Analysis

The research data regarding the main question of the paper is qualitative and will be primarily acquired from many sources. The validity of the information is medium to high, due many than one sources explaining the subject through numerous ways, but the main certainty comes from official documents from International Maritime Organization, Cybersecurity and Infrastructure Agency, and the maritime cyber security guidance book from Gary Kessler.

Research Subject and Its Following Inquiries

The research topic is described as follows: Cyber Threats That the Maritime Industry Currently Face Around the Globe.

Main question: What Are the Current and Potential Threats That the Maritime Industry Will Likely Face in the Cybersecurity Sector?

Firstly, an established knowledge of what Maritime Transportation System is, and its different components that affiliate to one another to make Maritime Transportation System operational is needed to comprehend the main question of this paper. Furthermore, the paper will also discuss the definition of all the common cyber-attacks that have happened to the Maritime Transportation System, including the officially known cyber-vulnerabilities of the Maritime Transportation System that is still present until now. By understanding all the subjects mentioned above, the readers will hopefully understand the current and potential cyber-threat of the Maritime Transportation System and will further develop cyber-awareness to help protect the maritime industry from the cybersecurity perspective.

From here, the theme will be divided in four sub enquiries. In doing so, it will then create way of understanding the topic as well as creating knowledge about the subject. All those sub questions are included in the following:

- What encompasses the Maritime Transportation System around the world?
- How do ships operate in open water and how dependent are they to the modern-day technology?
- What are some of the most common cyber threat vectors that the maritime industry is currently facing?
- What are the most prevalent cyber vulnerabilities that the maritime industry presently has?

Research Result

Research Question #1: What encompasses the Maritime Transportation System around the world?

Maritime Transportation System (Joe Webster, n.d.) is the shipment of cargo and people by sea, oceans, canals, and other waterways, and it is highly reliant on information communication technologies. The Maritime Transportation System itself comprises of six main domains, in which in every aspect of these domains are dependent on information communication technologies. All six of the Maritime Transportation System domains are described in the following, as well as some parts from the domain that are reliant on information communication technologies (*For more comprehensive detail surrounding the MTS ecosystem, see Figure 6 in the Appendix*):

- **Ships** – in which they have navigation and communication systems, and shipboard networks.
- **Shipping Lines** – have reservation and scheduling, financial, and operation systems that are computerized
- **People** – have customers, vendors, and trading partners that use technologies
- **Ports** – have communication and traffic management, and logistics in which allow shipping containers to be identified when the ships are taken off, put on a truck, and be taken to their determined destination
- **Intermodal Transfers** – have airlines, railroads, and trucking.
- **Inland Waterways** – have ATONs (Aids to Navigation), which are personal navigation devices that are used to navigate the waterways, and these devices are digitized as well.

Furthermore, this paper will dive deeper into two domains which render the creation of the Maritime Transportation Systems, which are ships and ports, the later part being discussed on the next research question. When it comes to the word maritime, one usually associated it with ships. Ships (Drew, n.d.) are vessels larger than a boat used for transporting and carrying cargo, goods and/ or people (passenger) or supporting specialized missions such as defence, research, and fishing by the world's ocean, sea, canals, and other sufficiently deep waterways. Ships are the raison d'être of the Maritime Transportation System. Ships are commonly determined based from their sizes, shapes, load capacity, masts, factors in costs, number of decks, and purposes. They vary from one another based on their requirements, utilities, strengths, and weaknesses. Each ship was crafted with a different purpose in mind, and they require different numbers of sailors to oversee them. Currently, more than 50.000+ ships are in operation worldwide (The Engineering Post Team, 2022), doing their business around the world and carrying around 90% of all the goods, commodities, and products that people need. There are many distinct types of ships that have been made around the world, and this paper will only name few of the most well-known of them:

- **Passenger ships** – also known as cruise ships are primarily made for transferring passengers in transit from one place to another. Unlike seaplanes used for transportation, cruise ships are usually used for round-trip voyages to various ports, where passengers can go on tours. Modern types of passenger ships have less hull strength, speed, and agility than seagoing ships. These vessels are strictly required to follow inland water and sea travel regulations and can do two or three nights or more round trips without visiting any port. Passenger ships have two general sub-divisions:
    - **Ferries** – are used for transporting passengers on short distance routes
    - **Cruise ships** – are sea-going vessels used for leisurely and recreational activities and travel. They are descended from transatlantic ocean liners, which have seen their services supplanted by jet aircraft since the mid-twentieth century. Most of these ships travel to selected tourist destinations around the world. They are further classified as:
        - **Cruise ships, liners, pilgrimage ships**

    - **Artic and Antarctic cruises**
    - **Coastal, Harbour, and Cross Channel ferries**

- **Tanker ships** – are specialised vessel designed to carry and transport a large/ vast amount of stored liquid cargo or gases. Because of these ships are so enormous, they must berth on the open seas. They can hold up to two million barrels of oil. They are further classified into diverse types based on the cargo they carry:
    - **Oil tanker** – ships that carry crude oil and its by-products.
    - **Chemical and Product Carrier** – are chemical tanker ships that designed to transport chemical liquids and different other liquid products in bulk.
    - **Liquefied Gas Carriers** – are gas tanker (gas carrier) ships that carry liquefied gas, such as LNG (Liquefied Natural Gas), CNG (Compressed Natural Gas), LPG (Liquefied Petroleum Gas), or liquefied chemical gases in bulk.
- **Container ships** (*see Figure 10 in the Appendix*) – are built to accommodate and transport huge quantities/ amounts of cargo of goods in containers. These cargos are housed in metal containers that are arranged or compacted on the deck of the ship. Also, these ships can transport thousands of containers per trip. Some container ships only have one deck, while others can have multiple decks. These ships play a crucial role in international trade as they transport all kinds of items, including machinery, metals, furniture, clothes, food, and many more. **Refrigerated Container ships** are vessels that carry refrigerated cargo (in refrigerated containers). Container ships are also further categorized based on their size: Panamax, Suezmax, Post-Panamax, Post-Suezmax, and Post-Malaccamax.
- **Dredgers** – are the drafted sea craft to excavate a need for underwater soil. They are equipped with excavation tools used for removing sand, silt, gravel, and other types of deposits from the inlet streams, waterways, or the ocean floor/ seabed. Dredging is usually done in shallow seawater to collect the bottom sediments below for deep sea-mining, widen the water passageway to make shallow coastal areas navigational, etc. They are two general types of dredgers:
    - **Hydraulic Dredgers** – hydraulic system provide their excavation power
    - **Mechanical Dredgers** – their power of excavation comes from a mechanical gear system driven by powerful electrical motors
- **Ro-Ro (Roll-on Roll-off) Ships** – are carrier vessels designed to transport wheeled cargo, such as cars, buses, trucks, semi-trailer trucks, trailers, motorcycles, and railroad cars across international waterways. These wheeled vehicles are driven on and off a ship, either on their wheels or using a platform vehicle, such as self-propelled modular transporter. The fact that driving a vehicle onto the boat is safer and faster than employing a crane is one of the reasons these ships are so famous for transporting autos. They are in contrast with Lo-Lo (Lift-on Lift-off) ships, which use cranes to load and unload the cargo. Once on board, the cars are secured to the ship's deck to prevent them from rolling about while at sea. Ro-Ro ships have either built-in or shore-based ramps or ferry slips that allow cargo to be rolled on and off the vessel efficiently. The word Ro-Ro is used for large ocean-going vessels.
- **Offshore ships** – are vessels that help and are used in oil exploration and construction jobs at sea. The latter functionality being to transport goods and people for construction projects at sea. There are different classifications for offshore vessels:
    - **Drill ships** – are merchant vessel designed to be used in exploratory offshore drilling of new oil and gas wells. Geologists and scientists aboard these ships are looking for new well deposits either for scientific drilling or for commercial purposes.
    - **Semi-submersible Drill Rigs** – are mobile offshore drilling machines that build stable and sturdy platform for oil and gas drilling operations
    - **Driving Vessels** – are the class of ships used by divers as they accomplish their underwater jobs in the sea.
    - **Supply Ships** – supply goods and materials to offshore rights.

  - **FPSO (Floating Production Storage and Offloading)** – these vessels function as storage units. There are also offloading vessels used in the gas and oil industry that produce and process hydrocarbons, including oil storage.
  - **FSU (Floating Storage Unit)** – these vessels are used solely for storing oil and its by-products.
  - **Accommodation Barges** – these watercrafts are used to accommodate people and cargo. They can also be used as stand-alone floating hotels.
  - **Pipe Layers** – are used by pipe and cable workers to lay pipes and cables underwater
  - **Anchor Handling Vessels** – are used for offshore construction and installation operations
  - **Production Platforms** – are used in the extraction and processing of natural gas and oil. They can also be used as temporary storage units of oil and gas until they can be transported to shore for refining, processing, and marketing.
  - **Crane Barges or Floating Cranes** – are equipped with huge cranes designed to lift heavy loads.
- **Fishing vessels** – are averaged-sized ships that are primarily used for catching fish or other marine wildlife. They use a conical net that traps fish by dragging it through or down the water and into the net. They serve many purposes of fishing, including professional, recreational, commercial, artistic fishing, or leisure cruising. They can be used for fishing at sea, on a lake, or in a river, as the name suggests. The total number of fishing vessels in the world in 2016 was approximately 4.6 million (The Engineering Post, 2022).
  - **Factory ships** – function as fish processing vessels. They are the big ocean-going vessels with all extensive necessary onboard facilities for freezing and processing caught fish of all sizes, including whales.
  - **Purse Seiners/ Trawlers** – fishing trawlers also called draggers, are the commercial fishing vessels designed to operated fishing trawls. Trawling is a method of fishing that involves actively dragging or pulling a trawl through the water behind one or more trawlers.
- **Naval ships** – are ships designed for military service used by the navy. They are large ships built differently from civilian ships by construction and purpose. Because of their intended use, they are designed to confront and engage opposing enemy forces on high seas, including distinct types of battleships, destroyers, and corvettes. They are also made with stronger materials so that they can resist damage from outside forces. In general, these ships are armed and outfitted with weapon systems and weapon framework, although the deadly implement on military transport is light or non-existent. There are naval ships fundamentally designed for maritime fighting and naval warfare and are called warships. Ships made for support functions are called auxiliary ships. These ships are intended only for shipyard operations and seldomly used for troop and armament transport.
- **Special purpose ships** – are constructed and used for specific purposes. Several types of ships include as follows:
  - **Ice breaker ships** – are used for cutting or breaking ice deposits in extremely severe cold climate conditions to make waters navigational for vessels
  - **Research vessels** – special types of vessels used to conduct a variety of research at sea. Some of the most known types of these ships are seismic, hydrographic, oceanographic, and polar vessels
  - **Tenders** – are boats or larger ships used to service or support other boars or ships, to transport people and/or supplies to other ships or boats at sea.
  - **Timber carriers** – vessels that carry and transport logs or timber.

Research Question #2: How do ships operate in open water and how dependent are they to the modern-day technology?

System On a Modern Cargo Ship (*see Figure 1 in the Appendix*). A ship itself comprises on different systems that are interconnected by one form of communications network or another, such as:

- **The ship network** – includes communications with customs and immigrations, e-mail facility and timekeeping.
- **Navigation** – including GPS, radar, and Electronic Chart Display and Information System.
- **Updates and Remote Access** – function as means to updating the computers of the ship and remote access to many of the systems including third parties.
- **Communication systems** – this includes the AIS, radio, ship-to-shore VoIP, and satellite link
- **Crew network** – is a separate network for the crew of the ship that might include e-mail, entertainment, and wi-fi/ wired network.
- **Network backbone** – is for all computing devices which includes the CCTVs, firewall/ internet, intercom system, master clock.
- **Industrial Control System**– are cyber physical systems that control things such as cargo handling, propulsion/ steering which is important to the navigation of the ship, human-machine interface, and Operational Technology
- **Loading and Stability** – that is provided by the exclusive information technologies of the ship.

Ports themselves are where ships dock and cargo and people are loaded and unloaded, whereas ships transport cargo and people. They are a diverse ecosystem consisting of many interrelated entities. Below is an explanation of what part of a port is called and what are their functions with a regard to the picture (*see Figure 3 in the Appendix*):

1. **Terminal gate** – is a secure entry point that is usually staffed with guards, CCTVs, and alarms that are connected to a computer network. Passengers, employees, cargos, and supplies enter to the gate before being loaded onto ships.
2. **Terminal** – comprises information and communication technology systems at the port. Malign actors will seek to attack by compromising these computer systems to access client, employee, ship, or cargo information.
3. **Terminal headquarters** – malign actors can disrupt the information communication technology through the disruption of these systems. They can overwhelm the headquarters through a DoS attack which would knock these systems offline and thereby all port activities. Because ports have incoming and outgoing vessels destined for other locations, the disruption of one area of a port can descend to incoming vessels and to other ports as well.
4. **Industrial Control System** – represents the cyber physical systems that are crucial parts of ports and ships. An ICS is a general term that describes distinct types of control systems and associated instrumentation, which include the devices systems, networks, and controls used to operate and/ or automate industrial processes. Regarding the port, an Industrial Control System is used to measure and control valves, pumps, cranes, propulsion systems, and cargo handling. A compromised ICS can interrupt or shut down port operations, cause physical damage to cargo or equipment, or result in injuries to the employees.
5. **Position, Navigation, and Timing (PNT)** – refers to systems used for port logistics and navigation. These systems can be knocked offline through spoofing or jamming.
6. **Vessels or Modern Ships** – are floating computers and networks and the reason of ports' existence. Malign actors' targets include ships picking up and delivering cargo, and/ or passengers and other vessels as well. An attack on a shipboard computer has the capability of not only affecting other device networks on the ship, but landslide communication systems as well. This will then result in cascading effect on incoming and outgoing vessels as well as other ports.

Research Question #3: What are the most common cyber vectors that the maritime industry is still currently facing?

Cyber threat vector is a path or means by which a malign actor could gain access to a computer or network through one or more routes into a computer system or network by exploiting a vulnerability.

Cyber threats can be categorized into two kinds of categories:

- **Intentional cyber-incidents** are the result of hacking or malware. Malicious hackers or disgruntled employees may perform these.
- **Unintentional cyber-incidents** are the result of operator misuse or design flaws. Some examples are poor software maintenance, software bugs due to lack of testing, or inappropriate user permissions.

Unintentional cyber threats tend to be caused by a human error by the form of misunderstanding of between the crew's communication. For this paper, it will dive specifically at intended cyber-incidents normally caused by a malign cyber actor. Firstly, to get through a network there are several different routes for the malign actors to take, including the network itself, users, e-mail, web applications, or remote access portals. Some of the most common cyber threat vectors that have happened to the maritime industry are information leakage, intellectual property theft, GPS and AIS spoofing and jamming, ransomware, and phishing.

Phishing attack is practice of sending fraudulent communications that appear to come from a trusted reputable person, organization, or source that lure unknowing victims as an attempt to obtain data that are sensitive like username, password, and more. It is the most common social engineering attack. Social engineering is a psychological manipulation of people into performing actions that divulge confidential information. It is usually done through e-mails. Phishing is an umbrella term for several types of social engineering attacks, and a social engineering attack can occur through any medium, including text messages, phone calls, regular mail, face-to-face, and e-mails. Phishing attacks are one of the most common cyber-attack vectors across both government and industry. The goal of the cyber actors is to use social engineering to dupe unsuspecting victims to react to the contents of the e-mail. It only needs as simple as a single click on the button of the e-mail that was sent, and it will redirect the computer to a web browser on the internet that is using a less secure protocol, the computer then proceed to install a malware that has been scripted to be downloaded automatically without the user's acknowledgement or consent. The easiest way to spot if an e-mail is directly sent from a trusted source is to hover the mouse pointer above the button to see where it is going to. An e-mail containing promotion code from Amazon should lead to a link that has Amazon.com on its initial. The content of the e-mail is usually trying to engender a sense of urgency which will create a psychological manipulation.

Ransomware is a malware that encrypts data on a storage device. It has been indicated as the current greatest cyber threat delivered through phishing e-mails by the FBI (IC3 Report, 2019). The encryption is sufficiently strong that files cannot be decrypted without decryption key. Once the ransomware encrypts the files, a message is presented to the user that explain what has occurred (ex. The user's files have been encrypted), and how to purchase a decryption key using some form of anonymous cryptocurrency so that there can be no attributions back to the identity of the threat actors (Linda, Lindamood-Craiger, & Zori, 2021). The actual malware that infects the host computer and encrypts files often arrives in the form of a legitimate appearing attachment to an e-mail (ex. Invoice). Once the attachment is clicked by the user, the ransomware silently starts the encryption process; the user is normally unaware of the encryption running, until it is already too late.

A notable example of this type of attack that has happened is the Maersk 2017 incident being hit by NotPetya malware (Bialas, 2021). Maersk is a Danish shipping company that. The numbers have yet to be reached to an agreement of determination, but it is estimated to be around $200-300 million.

Initially, the ransomware was executed on a single computer on the Maersk network. It then quickly spread across the global IT infrastructure, encrypting hard drives across 170 Maersk global offices, forcing the recovery efforts to the entire IT infrastructure, including installing software and files on over 4.000 servers, 45.000 personal computers, and 2.500 applications over 10-day period. NotPetya was originally a state-sponsored cyberattack by the Russians targeting at Ukrainian shipping companies, but it spread beyond the Ukrainian borders and caused estimated $10 billion damage in total worldwide. Port terminals in United States, India, Spain, and the Netherlands, all run by Maersk, experienced massive disruptions. Although the cargo container ship computers were not affected, it did not really make a significant difference, as the Maersk office computers, most of which contained the logistics programs and information on their supply chain, were inoperable. Even when the container ships were able to dock at a port, thousands of semi-trailer trucks at pick-up and distribute cargo were unable to collect their cargo, as there was no way of knowing which containers are on the ships, or the cargo that was inside. This is fitting example that states if one of the MTS systems (MTS system already explained in above question) is down, the effect will cascade on all other parts of the system because of the intimate connectedness of the Maritime Transportation System.

"Ghost shipping" attack is an actual instance of a cyber-attack on maritime transportation in the Netherlands. In this type of attack, sophisticated malign actors infiltrated a cargo shipping company's networked business logistics system to modify bill of lading information. To deepen the understanding of the description above, some of its key term will be described as follows. Business logistic is a business planning framework that is concerned with material procurement, materials management, and overall inventory control. It is an activity that takes goods from source to destination location. Bill of lading is a legal document issued by a carrier to a shipper that details the type, quantity, and destination of the goods being carried. It reserves as a shipment receipt when the carry delivers the good at a predetermined destination. All that information is contained computers and network throughout the business.

In the case in the Netherlands, the Dutch drug traffickers hid drugs inside shipping containers that were in route to Port of Antwerp (the largest port in the Netherlands). The malign actors gained access to the terminal systems that contained logistics information on the contents and owners of containers and modified that information. Logistics programs that the cyber actor managed to gain access to, contain information regarding hundreds of thousands of containers that each cargo ships of the company are responsible transporting to that are being run by shipping companies. When the ship docked at port the malign actors would then to collect their containers. Then the shipping companies would release the containers containing drugs to the actors based on false bill of lading documents, and this would happen before the rightful owners could take delivery of the shipments.

AIS and GPS spoofing and jamming (navigation attack on ships) is the type of attack where hackers either send false navigation information to the crew, seeing the vessel sail off course, or sending false information regarding the vessel's location to the shore-side team. Navigation system comprise of variety of devices that allow for the tracking of the current location of the vessel as well as set the future direction of the travel of the vessel. There are several parts of a ship's navigation, they are: AIS, GPS/ GNSS, autopilot, echo sounder, ECDIS, NAVTEX, Gyroscope, navigational workstation, radar, sonar, and various kinds of sensors (e.g., rate-of-turn, rudder, salinity, water temperature, and weather). AIS is a transponder that transmit course, speed, type of vessel, type of cargo, at-anchor or underway status, and other information for safety purposes, but this information is neither encrypted nor authenticated. And the reason this is still happening now is that the AIS protocol was designed at time before it was easy to create spoofed signals. There are mitigation solutions that would be able to encrypt and authenticate these AIS messages, however it would require the installation of new hardware on hundreds of thousands or even millions of thousands of ships.

Research Question #4: What are some of the most prevalent cyber vulnerabilities that the maritime industry still presently has?

Below are listed three of the most common target of MTS shipboard targeted by the unethical hackers (The Guideline on Cyber Security Onboard Ships, 2020, Chapter 3):

Ship-to-shore Connection (Digital Links). Ships are becoming more integrated with shoreside operations because digital communication is being used to conduct business, manage operations, and retain contact with head offices. Critical safety and navigation systems for power and cargo management have become increasingly connected to the internet to perform a wide variety of legitimate functions, such as:

- Engine performance monitoring
- Remote ships diagnostics
- Maintenance and spare parts management
- Cargo and container tracking and management, loading and unloading, and stowage planning
- Crane and pump management
- Monitoring of system for adherence to environmental regulations and reporting

Remote Access Connection Between Ships. Ships are connected via the internet to their home offices landsite. Therefore ship-board systems are remotely accessible and may operate with continuous internet connection for remote monitoring, data collection, maintenance functions, safety, and security. These systems can be "third party system," whereby the contractor remotely monitors and maintains the systems. The systems may include a two-way data flow and/ or upload-only functions. System and workstations with remote control, access or configuration functions could be:

- Bridge and engine room computers and workstations on the ship's administrative network
- Hull stress monitoring systems
- Engine monitoring and control
- Safety and security networks, such as CCTV

Ship visits. Lastly, there are third party ship visits. They require a connection to one or more computers on board and can also result in connecting the ship to shore via the internet. Commonly technicians, vendors, port and other officials, marine terminal representatives, agents, pilots, and other technicians to board the ship and plug-in devices, such as laptops and tablets. Some of the technicians may require the use of removable media to update computers, download data and/or perform other tasks. Removable media (Virgillito, 2020) is another terrific way for a ransomware to sneak into devices using USB flash drive and memory sticks. Cyber threat actors inject malware into removable devices and wait for unsuspecting users to connect to them to their systems. This counts as a risk as if a user's system is connected to an enterprise network, it could allow the ransomware to infect a whole organization.

Furthermore, below are some of the most common cyber vulnerabilities, which may be found onboard existing ships, and on some newbuild ships (The Guideline on Cyber Security Onboard Ships, 2020):

- Obsolete and unsupported operating systems.
- Outdate or missing software protection from malware.
- Inadequate security configurations and best practices, including ineffective network management and the use of default administrator accounts and passwords, and ineffective network management which is not based on the principle of least privilege.
- Shipboard computer networks, which lack boundary protection measures and segmentation of networks.
- Safety critical equipment or systems always connected with the shore side.
- Inadequate access controls for third parties including contractors and service providers.

Conclusion and Discussion

Conclusion

The Maritime Transportation System is highly reliant on information communication technologies, and it will continue to do so as the era progresses to becoming more modernized. The Maritime Transportation System itself is an extraordinarily complex domain consisting with many types of assets, operations, and infrastructure as well a widely diverse set of stakeholders. From a system's perspective, the Maritime Transportation System is a network of maritime operations that interface with shoreside operations at intermodal connections as part of overall global supply chains or domestic commercial operations. When one system falls to a cyber-attack, this could result in devastating cascading effect on to other systems as well. Because of its nature that highly dependent on information technologies, this will make the Maritime Transportation System very susceptible to cyber-attacks from malign actors. The Maersk incident is a good example of this as it demonstrated the fragility of these systems, and the need to ensure cybersecurity. And looking towards the future, with the development of fully automated ships, the maritime companies really need to start implementing cyber safety to all aspects of their IT and OT infrastructure.

In general, there are two categories of cyber threats that may affect companies and ships:

- Targeted attacks – where company or ship's systems and data are the intended target or one of multiple targets.
- Untargeted attacks – where company or a ship's systems and data are one of many potential targets.

These attacks are likely to use tools and techniques available on the internet, or more sophisticated tools and techniques that are made for targeting a certain company or ship, which can be used to locate, discover, and exploit widespread vulnerabilities that may also exists in a company and onboard ships.

Therefore, below are listed the target/ attack vectors that currently mark the Maritime Transportation Systems that may affect companies or ships (BIMCO, 2020):

- Social engineering – a non-technical technique used by potential cyber-actors to manipulate insider individuals into breaking security procedures, normally, but not exclusively, through interaction via social media.
- Phishing – which is a part of social engineering. It is an activity of sending e-mails to large number of potential targets asking for particular pieces of sensitive or confidential information.
- Ransomware
- Water-holing – the use of establishing a fake website or compromising a genuine website to exploit unsuspecting visitors.
- Scanning – searching for substantial portion of the internet at random for vulnerabilities that could be exploited.
- Spear-phishing – which also counts as a part of social engineering. It is just like phishing, but the individuals are targeted with personal e-mails, often containing malicious software or links that automatically download malicious software.
- Deploying botnets
- Subverting the supply chain – attacking on a company and ship by compromising equipment, software or supporting services being delivered to the company or ship.

In broad overview, below are listed some of the most common MTS targets, in specifically the ship domain, of cyber-attacks by malicious actors throughout the course of history (ASTM-F3286, November 02, 2018):

- Cargo management systems
- Bridge systems
- Propulsion and machinery management and power control systems
- Access control systems
- Passenger servicing and management systems
- Passenger facing public networks
- Administrative and crew welfare systems
- Communications systems

Some of the aspects particularly relevant to equipment and data onboard ships that if overlooked by the company, could lead to potential disaster to ships are including, but not limited to (Stephenson Harwoord, 2015):

- Computer access for visitors – if not managed correctly, a visitor can simply plug in USB drive into the ship's computers and will introduce malware onto the ship's administrative network.
- Crew's personal devices – untrained personal crews could utilize a ship's communication network for personal and leisure purposes by the means of IT devices.
- Anti-virus and anti-malware tool management – without procedural requirements, it is often difficult to ensure updates are distributed to ships on timely basis and that all relevant computers are on board are updated. These tools are necessary to be kept up to date as they provide the means of scanning to detect and deal with malware.
- Multi/ factor authentication (MFA) and passwords – a frail password can increase the chances of brute force attacks, along with avoiding the risk of password being written on a piece of paper and kept near the computer. An MFA password is based on something that the owner of the password has, e.g., a token, or a device, something that the owner knows, e.g., personal information such as pet's name, or something that "the owner is," e.g., fingerprint passcode on a phone.
- Physical and removable media controls – when transferring data from uncontrolled systems to controlled systems, there is a risk of introducing malware. Removable media can be used to bypass layers of defences and attack systems that are otherwise not connected to the internet. However, there are situations where it is unavoidable to use these media devices, for example during software maintenance.
- Equipment disposal including data destruction – obsolete equipment can contain data, which is commercially sensitive or confidential. Should the company does not ascertain the proper destruction of the obsolete equipment, the data could be retrieved.
- Use of administrator privileges – administrative privileges allow full access to system configuration settings and all data. Users logging onto systems with administrator privileges may enable existing vulnerabilities to be more easily exploited.

From all the descriptions above, it is summarized that the Maritime Transportation System still has many vulnerabilities that can be exploited and could lead to potential prominent maritime cyber incident.

Discussion

The research question #1 is answered from the fabrication of many different internet articles online, but the main guideline is from the IMO article of the same subject. Research question number #2 is heavily indoctrinated from *Maritime Cybersecurity: A Guide for Leaders and Managers* book from Gerry Kessler with several internet sources also considered. The answer to the research question number #3 is based on many articles outlining the infamously known cyber-incidents that have happened in the maritime world, as well as both YouTube and site articles online identifying and describing their characteristics and definitions. Research question number #4 is heavily based on three book sources, which are *The Guidelines on Cyber Security Onboard Ships* by BIMCO, *Maritime*

Transportation System, Security Recommendations for the National Strategy for Maritime Security by DHS, and *Cyber Supply Chain Risk Management* by Aeronautical University.

All the citations and references mentioned above can be seen on the Literature List chapter of the paper.

Appendix

Figure 1: 70% of earth's surface is water

Figure 2: Nearly 80% live on the coast or near the water

Figure 3: 90% of trade is through water

Figure 4: Nearly 100% of transoceanic data traffic is transmitted under water through undersea cable

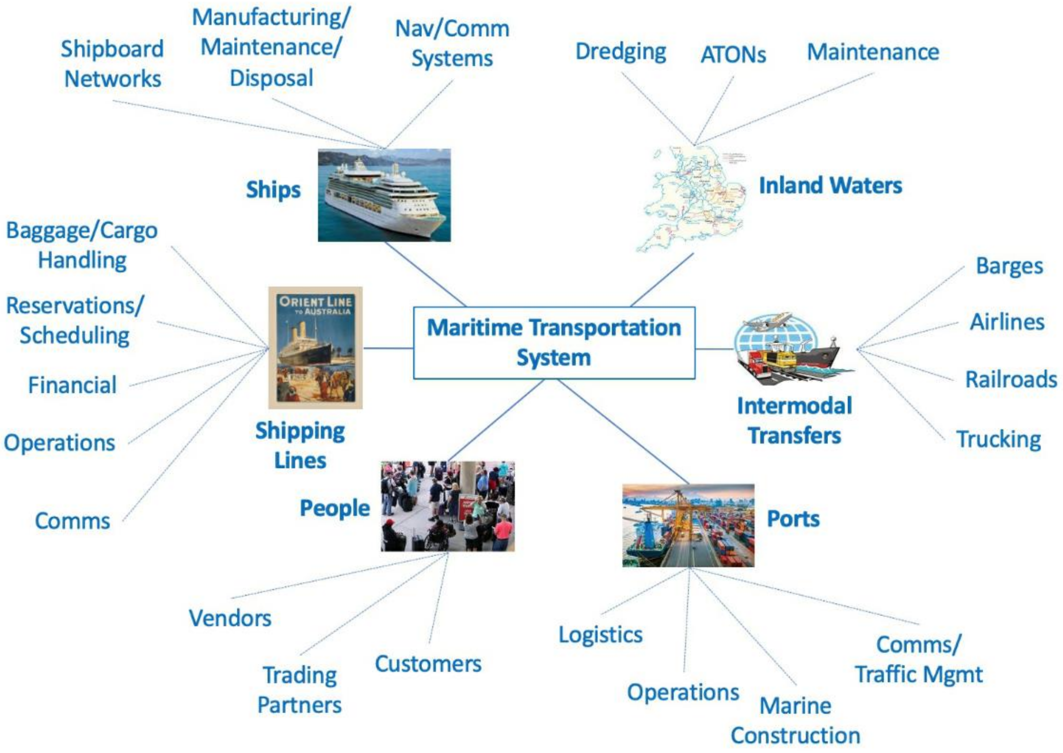


Figure 5: The MTS ecosystem (Kessler & Shepard, 2022)

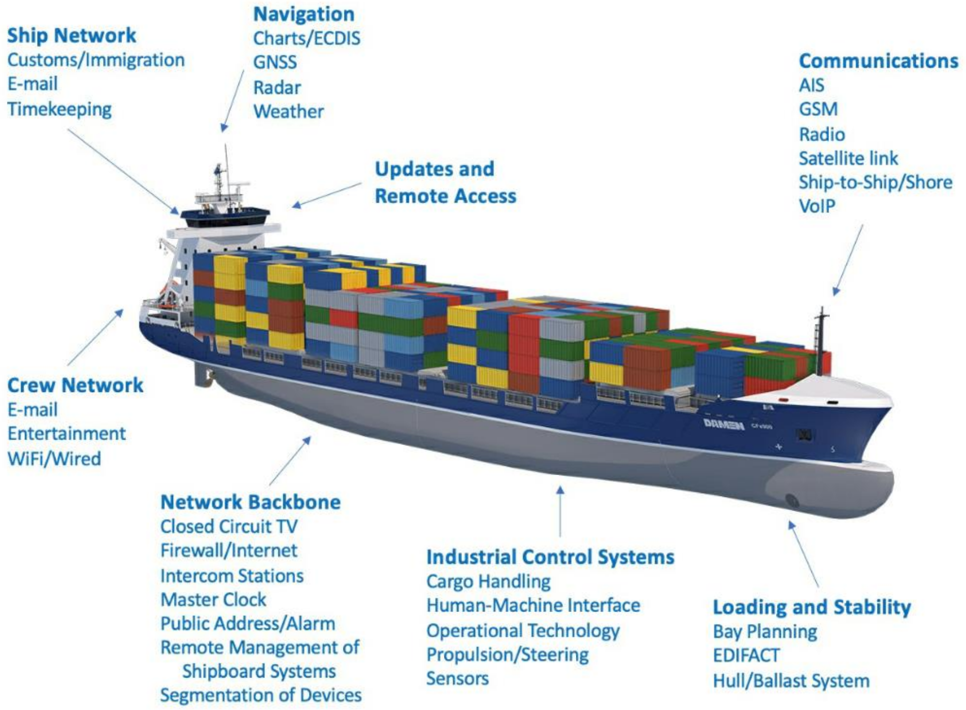


Figure 6: Modern container ship topology (Kessler & Shepard, 2022)

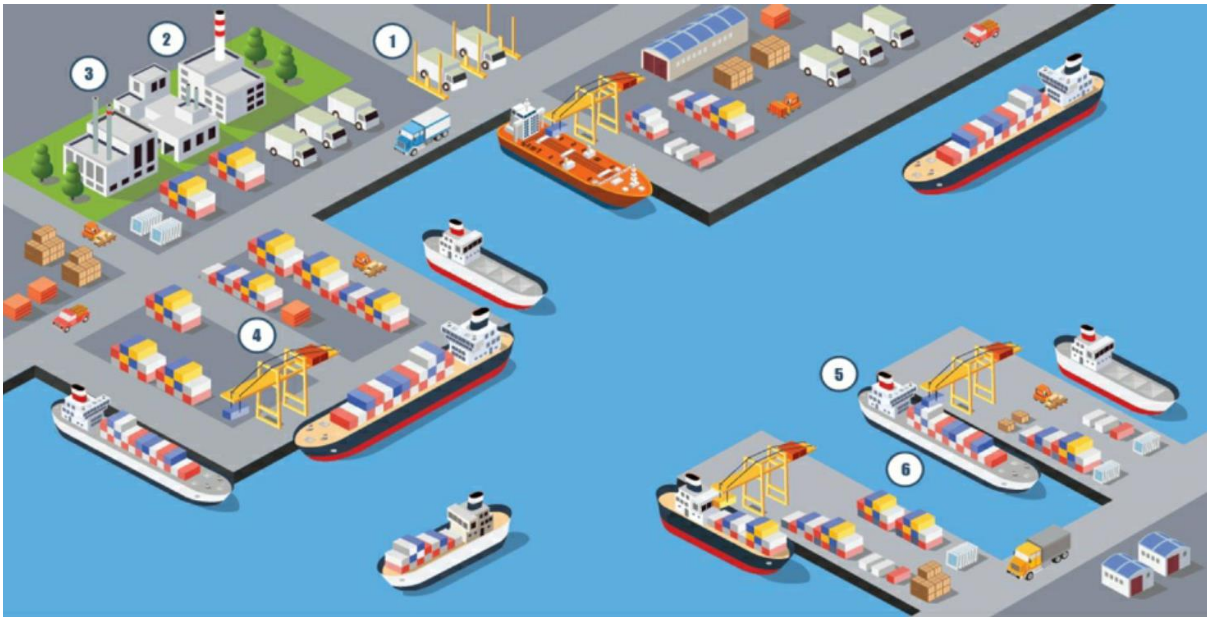


Figure 7: Different components of a port (Kessler & Shepard, 2022)

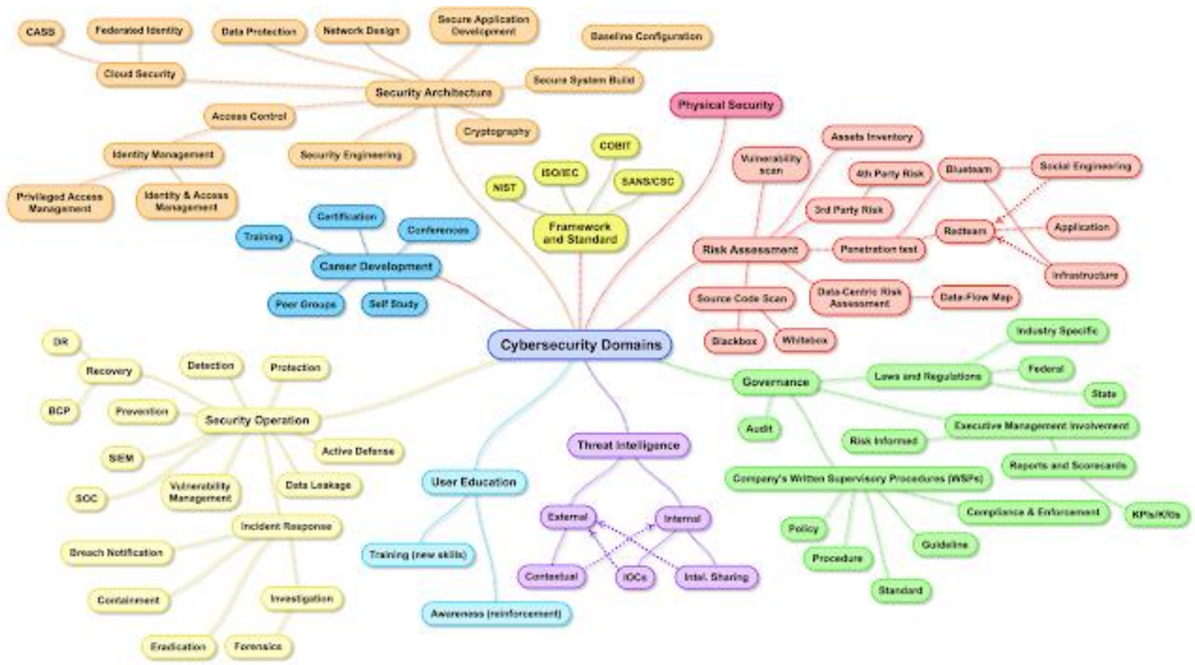
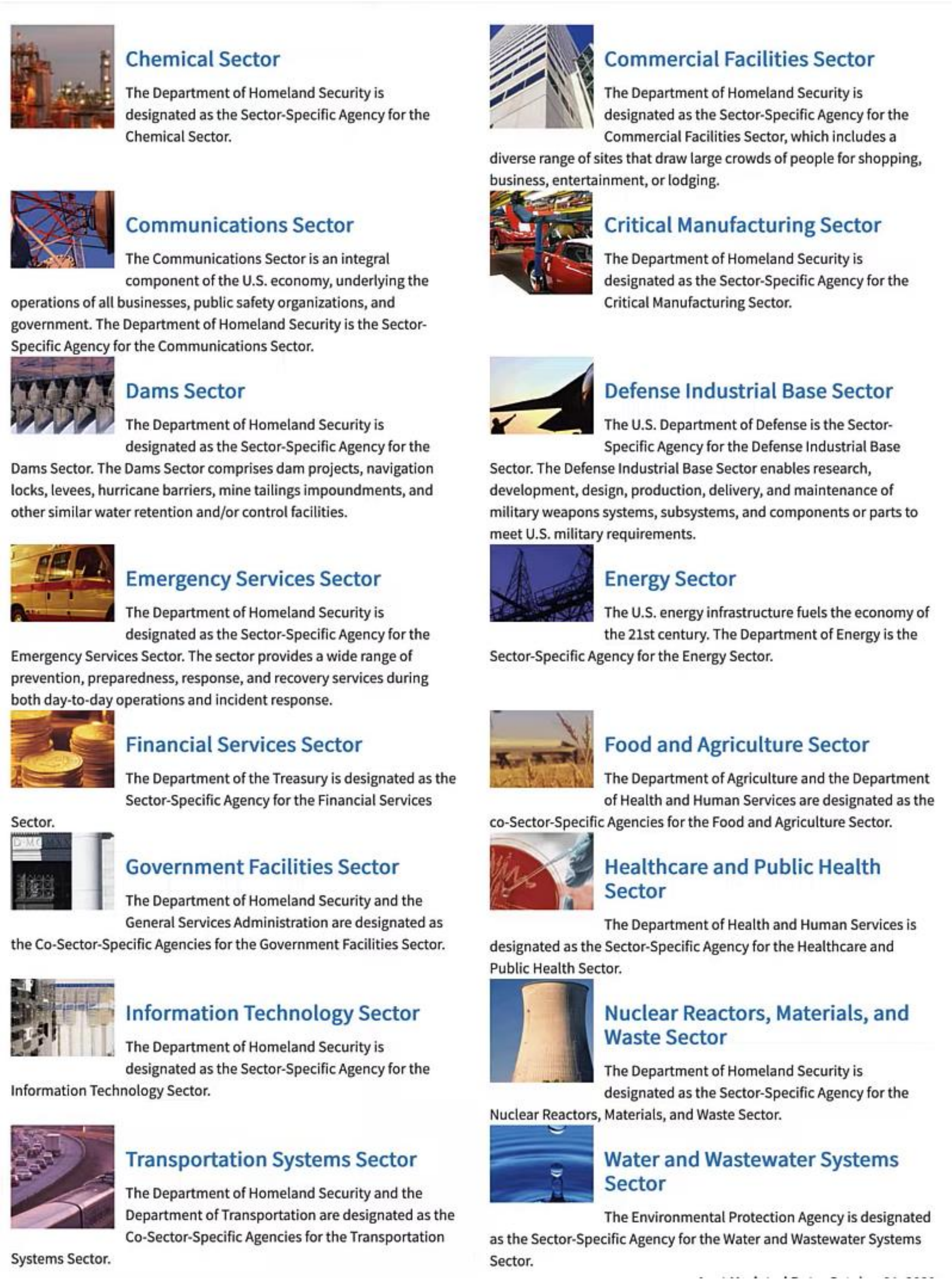


Figure 8: Cyber security domains (Henry Jiang, February 10, 2017)

Figure 9: Passenger ships (Boatinggeeks, n.d.).

Figure 10: Container ships (MarineInsight, August 1, 2021).



Chemical Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.

Communications Sector

The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. The Department of Homeland Security is the Sector-Specific Agency for the Communications Sector.

Dams Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Dams Sector. The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

Emergency Services Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Emergency Services Sector. The sector provides a wide range of prevention, preparedness, response, and recovery services during both day-to-day operations and incident response.

Financial Services Sector

The Department of the Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.

Government Facilities Sector

The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.

Information Technology Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.

Transportation Systems Sector

The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

Commercial Facilities Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector, which includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging.

Critical Manufacturing Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Critical Manufacturing Sector.

Defense Industrial Base Sector

The U.S. Department of Defense is the Sector-Specific Agency for the Defense Industrial Base Sector. The Defense Industrial Base Sector enables research, development, design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts to meet U.S. military requirements.

Energy Sector

The U.S. energy infrastructure fuels the economy of the 21st century. The Department of Energy is the Sector-Specific Agency for the Energy Sector.

Food and Agriculture Sector

The Department of Agriculture and the Department of Health and Human Services are designated as the co-Sector-Specific Agencies for the Food and Agriculture Sector.

Healthcare and Public Health Sector

The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.

Nuclear Reactors, Materials, and Waste Sector

The Department of Homeland Security is designated as the Sector-Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.

Water and Wastewater Systems Sector

The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.

Figure 11: All 16 critical infrastructure sectors defined by CISA (CISA, n.d.).

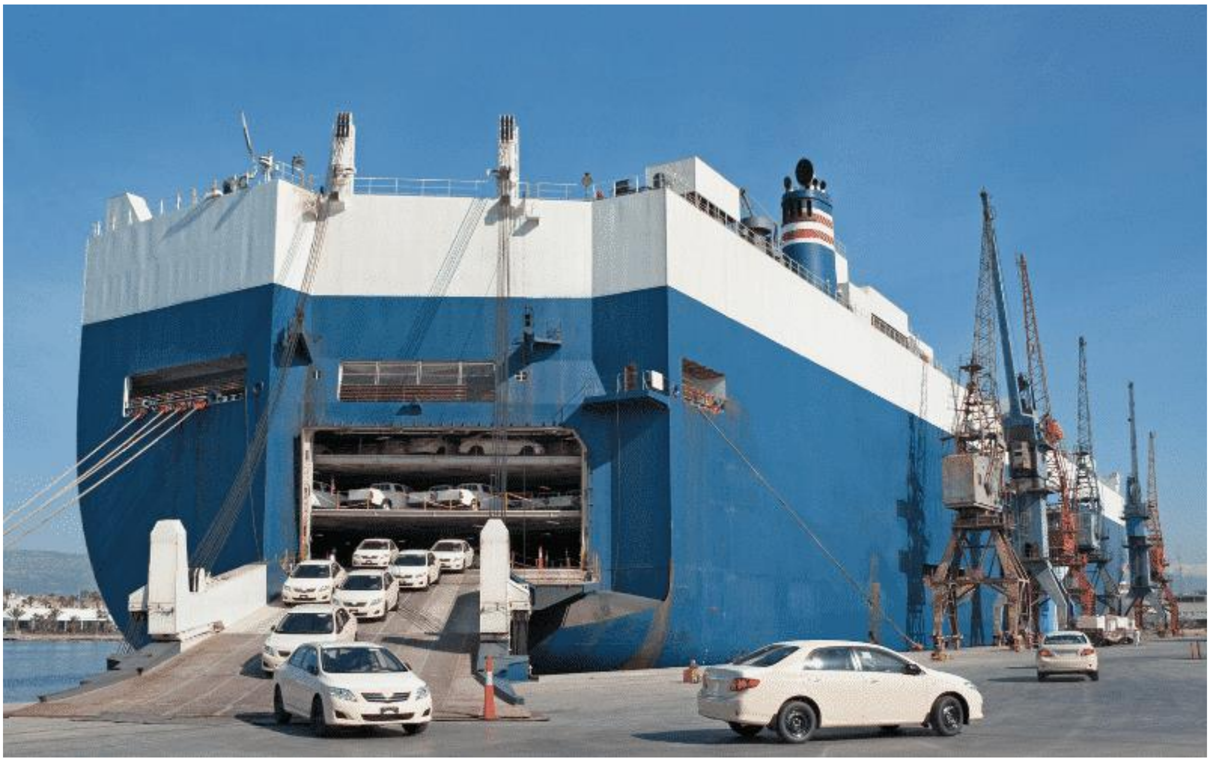


Figure 12: RoRo ships (MarineInsight, August 1, 2021).

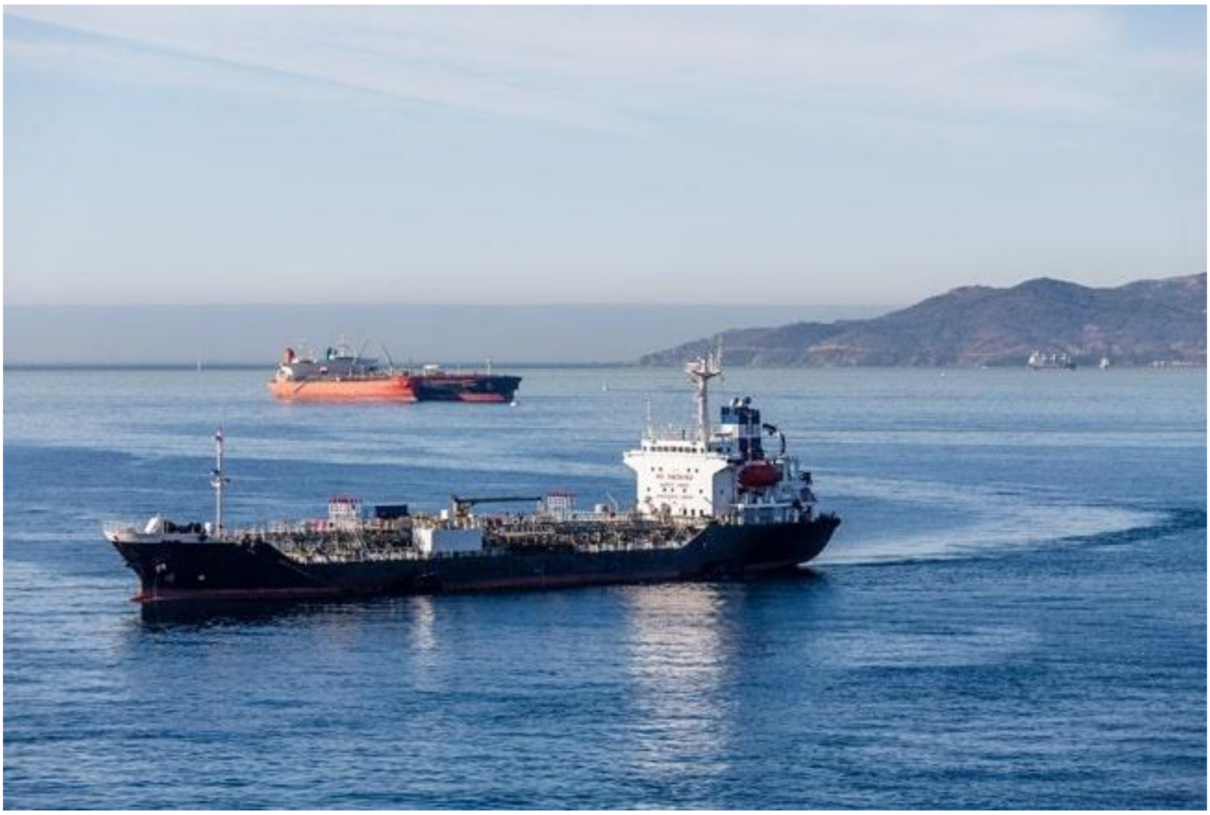


Figure 13: Tanker ships (MarineInsight, August 1, 2021).

Literature List

Agarwal, Mayur. (2021, July 29). *Different Types of Dredgers Used in the Maritime Industry*. MarineInsight. Retrieved on December 2nd, 2022, from https://www.marineinsight.com/types-of-ships/different-types-of-dredgers-used-in-the-maritime-industry/

Anonymous. (n.d.). *A Comprehensive Guide to Maritime Cybersecurity*. MissionSecure. Retrieved on December 9th, 2022, from https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach

Anonymous. (n.d.) *About Ship, Types of Ships, and What They are Used For*. IMO. Retrieved on December 20th, 2022, from https://kids.imo.org/en/about-ships.php

Anonymous. (n.d.). *Critical Security Controls for Effective Cyber Security*. CIS. Retrieved on December 23rd, 2022, from https://www.cisecurity.org/controls

Anonymous. (n.d.). *Types of Cargo Ships According to the Load They Carry*. SuiscaGroup. Retrieved on December 10th, 2022, from https://www.suiscagroup.com/en/noticias/types-of-cargo-ships-according-to-the-load-they-carry/

Anonymous. (n.d.). *Safety Regulations for Different Types of Ships*. IMO. Retrieved on December 21st, 2022, from https://www.imo.org/en/OurWork/Safety/Pages/RegulationsDefault.aspx

Anonymous. (n.d.). *Vessel Types Explained*. OneOcean. Retrieved on December 12th, 2022, from https://www.oneocean.com/news/vessel-types-explained/

Anonymous. (2018, November 02). *Standard Guide for Cybersecurity and Cyberattack Mitigation*. ASTMF3286-17. Retrieved on December 21st, 2022, from https://www.astm.org/f3286-17.html

Anonymous. (2019, October 15). *Types of Ships: Know When to Hire Each One*. WilsonSons. Retrieved on December 19th, 2022, from https://www.wilsonsons.com.br/en/blog/types-of-ships/

Anonymous. (2019, December 05). *Cybersecurity Rises to Surface of Maritime Industry*. Bezinga. Retrieved on December 16th, 2022 from https://finance.yahoo.com/news/cybersecurity-rises-surface-maritime-industry-211149000.html

Anonymous. (2020, August 17). *Real-World Lessons Learned from Maritime Cybersecurity Incidents*. MissionSecure. Retrieved on December 7th, 2022, from https://www.missionsecure.com/blog/real-world-lessons-learned-from-maritime-cyber-attacks-incidents

Anonymous. (2020, October 21). *Critical Infrastructure Sectors*. CISA. Retrieved on December 6th, 2022, from https://www.cisa.gov/critical-infrastructure-sectors

Anonymous. (2020, December 21). *5 Different Types of Ships That You Must Know*. MarineTreasury. Retrieved on December 16th, 2022, from https://marinetreasury.com/types-of-ships/

Anonymous (2020). *Ethical Hacking and Countermeasures – Complete Series* (11th ed.). EC-Council.

Anonymous. (2022, June 22). *20 Different Types of Ships and Their Functions [Images] Pdf*. TheEngineerPost. Retrieved on December 4th, 2022, from https://www.theengineerspost.com/types-of-ships/

Ball, Ben. (2020, November 12). *Why GPS Spoofing Is a Problem (And What to Do About It)*. Nextnav. Retrieved on December 3rd, 2022, from https://nextnav.com/gps-spoofing/

Bialas, Mateusz. (2021, August 25). *Maritime Cyber Attacks*. Vessel Automation. Retrieved on December 7th, 2022, from https://vesselautomation.com/maritime-cyber-attacks/

BIMCO et all. (2020). *The Guidelines on Cyber Security Onboard Ships* (4th ed.). World Shipping Council.

Black, Jessica F. (December 20, 2022). *What are the Different Types of Ships*. WikiMotors. Retrieved on December 11th, 2022, from https://www.wikimotors.org/what-are-the-different-types-of-ships.htm

Craiger, J. P., Zorri, Diane M., & Lindamood-Craiger, Laurie. (2021). *Cyber Supply Chain Risk Management: Implications for the SOF Future Operating Environment*. Aeronautical University.

Dimitriadis, Chris. (2019, July 18). *Modernized Maritime Industry Transport Cyberthreats to Sea*. Retrieved on December 15th, 2022, from https://www.csoonline.com/article/3410236/modernized-maritime-industry-transports-cyberthreats-to-sea.html

DHS et all. (2005, October). *Maritime Transportation System Security Recommendations for the National Strategy for Maritime Security*. Independently published.

Drew S. (n.d). *Types of Ships – Full List of 11 Different Types*. Retrieved on December 5th, 2022, from https://boatinggeeks.com/types-of-ships/

Gorham, Matt. (2020, February 11). *2019 Internet Crime Report*. FBI. Retrieved on December 8th, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf

Harwood, Stephenson. (2015, September). *Cyber Risk*. Joint Hull Committee in conjunction with the author.

Kessler, Gary C., & Shepard, Steven D. (September 2, 2020). *Maritime Cybersecurity: A Guide for Leaders and Managers* (1st ed.). Independently published.

Kessler, Gary C., & Shepard, Steven D. (2022). *Maritime Cybersecurity: A Guide for Leaders and Managers* (2nd ed.). Independently published.

Lucas. (September 8, 2021). *10 Types of Cargo Ships and What Makes Them Unique?* MICDOT. Retrieved on December 16th, 2022, from https://micdot.com/types-of-cargo-ships/

Raunek. (2021, August 1). *A Guide to Types of Ships*. MarineInsight. Retrieved on December 18th, 2022, from https://www.marineinsight.com/guidelines/a-guide-to-types-of-ships/

Rider, David. (2019, October 16). *Maritime Meets Cyber Security*. The Maritime Executive. Retrieved on December 17th, 2022, from https://maritime-executive.com/blog/maritime-meets-cyber-security

Stilwel, James Joseph, & Woodward, John B (n.d.). *Types of Ships*. Britannica. Retrieved on December 13th, 2022, from https://www.britannica.com/technology/ship/Types-of-ships

Uwadiare, Jennifer. (2021, August 19). *11 Different Types of Ships*. WheelsInquirer. Retrieved on December 17th, 2022, from https://wheelsinquirer.com/different-types-of-ships/

Virgillito, Dan. (2020, September 22). *Top 5 Ways Ransomware Is Delivered and Deployed*. Infosec. Retrieved on December 1st, 2022, from https://resources.infosecinstitute.com/topic/top-5-ways-ransomware-is-delivered-and-deployed/

Webster, Joe. (n.d.). *What is Maritime Transport*. A-1AutoTransport. Retrieved on December 23rd, 2022, from https://www.a1autotransport.com/what-is-maritime-transport/

Wilkinson, Ryan. (November 17, 2022). *Top 10 Different Types of Ships and Their Uses + Images*. Emozzy. Retrieved on December 15th, 2022, from https://emozzy.com/different-types-of-ships-their-uses-images/

Youd, Frankie. (2021, June 23). *Cyber-Attacks: How Hackers Are Targeting Seafarers*. Ship-Technology. Retrieved on December 3rd, 2022, from https://www.ship-technology.com/analysis/cyber-attacks-how-hackers-are-targeting-seafarers/