Maritime Ports and Cybersecurity

Kristen Kuhn, Jeptoo Kipkech and Siraj Shaikh

Original citation:
'Maritime Ports and Cybersecurity', in *ICT Solutions and Digitalisation in Ports and Shipping*, ed. by Michele Forini and Natalie Gupta, pub 2021 (ISBN 978-1-83953-086-9)

Publisher: IET

Maritime Ports and Cybersecurity

Kristen Kuhn,[1] *Jeptoo Kipkech*[1] *and Siraj Ahmed Shaikh* [1,2]

Maritime ports play a vital role in global trade. Goods are loaded at a port, transported, and unloaded at another port. Each port serves as a node in a global supply chain, which shapes trade and links states, economies, cultures, and the unknown.

In many ways, maritime ports resemble cyberspace, which also facilitates trade and serves as a connector. Like the internet, the ocean- vast and deep- is a source of prosperity and peril. It can be understood, then, why like the sea, cyberspace has recently been declared by NATO as a new domain of warfare [1]. The modern port exists in both sea and cyberspace, where these two domains of warfare overlap. The port is a physical infrastructure that faces traditional risks such as occupation. It is also a cyber-entity that faces new risks such as information leakage. While the traditional risks in ports have changed little, cyber-risks are a new and growing threat. In 2013, cyber-incidents were the 15th leading global risk for organizations and, in 2019- six years later- they were ranked second [2].

While cybersecurity threats and vulnerabilities are being addressed in the port industry, this has not been achieved to the degree required. This is in part because ports vary in structure and ownership, making standardization and regulation a challenge. Further, cyber-risk is multiplied by the connectivity of information, communication and cyber-physical systems, by which an isolated cyber incident in a port may have cascading effects across the global port system. To be effective, cybersecurity must evolve rapidly and constantly alongside technology implemented in ports.

This chapter introduces the modern port in Section 1.1 and explores its importance in Section 1.2. It then presents cybersecurity in Section 1.3 and draws a connection between ports and cybersecurity in Section 1.4, highlighting ports as a cyber-physical environment. To illustrate the cyber-threat landscape, five known attacks in ports are explored in Section 1.5. This chapter then examines control mechanisms in place for cyber-risk management for ports in Section 1.6 and reviews current cybersecurity guidelines and standards in Section 1.7. These concepts are encapsulated in the summary presented in Section 1.8, which mentions digital trends and the future of maritime ports and cybersecurity.

[1] Systems Security Group, Institute of Future Transport and Cities (IFTC), Coventry University, Coventry CV1 5FB, United Kingdom

[2] Security, Risks Management and Conflict (SEGERICO) Research Group, Universidad Nebrija, 28015 Madrid, Spain

1.1 The modern port

A *port* is a shore-based installation for the dispatch of cargo between land and sea [3]. There are many different types of ports, all of which can be classified as either sea, lake, river, or canal, depending on the type of business transacted [4]. For the purpose of this chapter, which deals with maritime ports and cybersecurity, "ports" refers to seaports. This section explores the port system in Subsection1.1.1, port ownership models in Subsection1.1.2, and port structure in Subsection1.1.3.

1.1.1 Port System

In medieval times, a "port" referred to a shore-based town whose main activity was trade [5]. A port had a harbor and could be recognised by characteristic infrastructures, including dockyards, warehouses and customs houses. With time, the port attracted other forms of commercial and industrial infrastructure, such as banks, agencies, and markets. These, in turn, attracted nearby goods and more extensive services, thus the town expanded. This can be viewed in light of the *central place theory*, which identifies such towns as geographical centers for markets and services [6]. These large towns then became cities, many of which today are major cities with a high concentration of civilians [7].

As port cities expand, so does the scope of their trade. Many necessities, along with secondary needs that sustain economies, are imported and exported by states through commercial ports. Ports which before were isolated or limited in trade became part of a complex, interconnected transport network. At this point, it makes sense to combine the central place theory with the *network theory* [8]. The network theory views ports not only as geographically relevant centers, but as functionally relevant centers whose value lay in their links to other ports and transportation systems. The growth of ports relate to the degree they are interconnected and interdependent on other ports from multiple states [5]. This is the modern port system.

The modern port is a multi-modal distribution hub which links transport by sea, river, road, rail and air routes. For many nations, ports are the main transport link with their trading partners and thus a focal point for motorways and railway systems [9]. This transport network is often referred to as the global supply chain. It is worth noting that in this network, ports themselves became a service in the mentioned chain. Take the case of Singapore, a major city which is also home to the world's second busiest port container terminal [10]. For a small nation like Singapore with few natural resources or agricultural industry, the port itself is a fundamental economic asset and its security is essential to the nation's economic well-being [11].

1.1.2 Port Ownership Models

There are various models of port ownership, the basic forms of which can be viewed on a scale of public to private ownership, seen below in Table 1.1.2. On this scale, ports are classified into four models: service port, tool port, landlord port, and private port [12]. However, the modern port is often a combination of these categories [9].

Public ownership can be associated with a *Port Authority*, which is a government or private body that is responsible for port administration, construction and management, and sometimes responsible for port operations and security [12]. Ports authorities may be established at all levels of government: national, regional, provincial, or local. Likewise, private ownership can be associated with a *Port Operator*, which "typically pursues conventional micro-economic objectives, such as profit maximization, growth, and additional market share" [12]. Port operators include terminal operators, cargo handling companies, and dockworker firms.

Table 1.1 Four port ownership models are shown from most public to most private. Their orientation relates to ownership of infrastructure, superstructure, dockworkers, and other functions. An example for each model is given.

Type	**Infrastructure**	**Superstructure**	**Dockworkers**	**Other functions**
Service Port	Public	Public	Public	Mainly public
	The Port of Colombo, in Sri Lanka is a service port. It is publicly managed: the port owns, maintains and operates every asset. Service ports are often run by the ministry of transport, and cargo handling is managed by the port authority. Service ports are in decline as many ports shift to landlord ports.			
Tool Port	Public	Public	Private	Mainly public
	The Port of Chittagong, in Bangladesh is a tool port. The Port Authority owns and operates the port infrastructure and superstructure, and makes them available to port operators. This can lead to conflicts regarding split of responsibility as the port authority owns and operates the cargo handling equipment, but the private cargo handling firm usually signs the cargo handling contract with the cargo owner or shipowner.			
Landlord Port	Public	Private	Private	Mainly private
	The Port of Singapore, in Singapore is a landlord port. It combines state and private ownership[1]. The port authority, or landlord, provides infrastructure and the port operator, or tenant, provides super-structure[1]. The port is split into terminals, which are leased for a set period of time. This is the dominant model in large and medium ports, and is the most common growing model.			
Private Port	Private	Private	Private	Mainly private
	The Port of Southampton, in the United Kingdom is a private port[2]. This is the only model where port land is owned privately and is rare as full privatization may be considered extreme. It implies a transfer of land, and often regulatory functions, from public to private ownership. This poses a risk in that the port can be sold for non-port activities or raise security concerns.			

[1] Alderton [9]
[2] Monios [13]
Source: The World Bank [12].

1.1.3 Port Structure

In ports, cargo can be transferred between land and sea by two methods: ship gear or quay cranes [3]. Ship gear is managed by seafarers and accompanies the ship from port to port. Quay cranes are managed by *dockworkers*, or labourers who load and unload vessels, and are part of either the port infrastructure (e.g. a paved terminal with deep-water access) or *superstructure*, which is built on top of the infrastructure (e.g. cranes and cargo-handling equipment) [9]. There is contention between using ship gear or quay cranes regarding the split of responsibility. That said, quay cranes are generally accepted as the more efficient of the two [3]. Beyond loading and unloading cargo which happens on the *quayside*, where land meets sea, port structure varies. The goods arriving at or departing for the port are moved by other cranes and vehicles, where they are either stored or moved onto other modes of transport, such as trucks or trains to *hinterlands*, or surrounding area.

Ports are constantly changing in response to diverse external factors- from weather to technology to political agendas. This renders every port unique in structure. This subsection explores how the physical structure of port is influenced by four factors: automation, cargo, ships, and transport network.

1.1.3.1 Automation

Most physical processes within ports, such loading and unloading cargo, are performed with automated or semi-automated mechanical systems and machinery (e.g. ships, trucks, cranes, electronic gates) under the control of sophisticated software systems (e.g. industrial cyber-physical systems, supervisory control and data acquisition [SCADA] systems, and surveillance systems) [7]. A controversial issue, automation draws tension between many actors. All can agree, however, that port automation- to be followed by automated vessels- marks a new industry standard.

The level of port automation has greatly increased the past couple of decades, with the ultimate realisation being the smart port. A *smart port* can be defined as a fully automated port where all devices are connected via the internet-of-things (IoT) [14]. Automation carves out early adapters as more efficient and safer than ever before. With that said, as ports become increasingly interconnected and reliant on automation, they become more vulnerable to a new threat: cyber risks.

1.1.3.2 Cargo

The decision to use ship gear or quay cranes also depends on the nature of the cargo. A ship may be carrying textiles or foodstuffs, petroleum, lumber, or hazardous goods. Special cargo arrives at terminals built to accommodate their storage requirements, e.g. grain is stored in silos; liquefied natural gas is kept in pressurized tanks. General cargo, however, is stored in container which arrives to a port container terminal (PCT). Containers are standard units adopted in the 1970's for transport of cargo on a global scale. This era is called containerization, and revolutionized transport. It also illustrates that ports must change in response to changes in cargo-handling technology [9]. Two external forces that had a prominent effect on cargo are standardization (containers) and globalization (goods passing through ports vary in type).

The standardization of shipping containers also gave birth to the *Twenty-foot Equivalent Unit (TEU)*, which is a key unit of measurement throughout the maritime industry [15]. The TEU is the standard unit of measurement for shipping containers, vessel size, and capacity- including how much cargo passes through a port, thus calculating port activity. For instance, top US ports Los Angeles and Long Beach handle over 16 million TEUs a year, while top ports in China Shanghai and Shenzhen handle over 65 million TEUs a year [15].

1.1.3.3 Ships

While the container is an industry standard for cargo, vessels that carry cargo are far from standardized. This presents a continuous challenge for ports, whose infrastructure must accommodate the ships they host. A quay crane, for instance, cannot unload a ship that is taller than it's own height. This challenge is greater still as ports last longer than ships. Most of the UK ports, for instance, were built between one and two centuries ago when ships were small [9].

In search of greater fuel efficiency and economies of scale, there is a tendency across the sector for larger vessels which move more good through ports faster, increasing productivity and profit [3, 16]. As container ships continue to grow, ports and port cities have adjusted to host them [17]. This concept was outlined in 1965: "The ports of the world are obsessed with the problem of handling more and larger ships; despite recessions in trade and financial ups and downs the management of our ports, whatever form their control may take, can never evade this problem" [3, 9].

Today, some container ships are nearly 400 meters long- the distance around an Olympic running track [17]. The rise of *mega-ship*, which can be defined as a ship with a capacity greater than 10,000 TEUs, took place in earnest as a response to the 2008 financial crisis [16]. Today, the mega-ship is challenging the port: The inability to expand because of a dearth of land suggests the end of the link between cities and ports [18]. Growing cities simply cannot accommodate growing ports, so there is a demand for special port complexes.

1.1.3.4 Transport Network

Since the design of ports and docks centuries ago, transportation has changed continuously, from horse and cart to autonomous vehicles [9]. The design and infrastructure of ports shifts according to vehicles and cargo-handling technology. The transport connections to a port also determines the geographic lay-out. For example, the warehouse storing goods may be situated near to tracks, with additional cranes that lift containers onto trains. The design of the port, and operational management, needs to be done so that congestion is minimized. The central place theory, which sees the port in a strictly spatial context, takes into account that growing ports infringe on cities- also growing- to occupy more space. However, this theory fails to account for other issues- such traffic congestion created from the port- which often also affects human mobility in surrounding areas [6].

1.2 The Importance of Ports

Cyber systems create benefits, but they also introduce risk. In the context of ports, *cyber risk* is the "probability of a threat agent exploiting a vulnerability to cause harm to a computer, network, system, or utility, resulting in financial losses, disruption or damage to the reputation of an organization" [19]. Risks to ports affect not only the ports themselves, but also their customers, stakeholders, and the global supply chain [19]. The risks can include, for example, financial loss, theft of cargo or information, strikes, and security malfunctions, which can lead to the shutdown of a port. This Section explores ports as critical infrastructures in Subsection 1.2.1, ports as critical information infrastructure in Subsection 1.2.2, and the impact of port disruption in Subsection 1.2.3.

1.2.1 Ports as Critical Infrastructure

Ports are a critical part of a national transport infrastructure [9]. *Critical infrastructure (CI)*, including ports, constitutes a probable target for cyber-attacks given its importance in the functioning of society [20]. Ports are especially vulnerable to cyber-threats as they are dependent on data systems, handle huge volumes of cargo and/ or passengers, process an immense number of transactions with high monetary value, and involve a wide range of stakeholders.

Through history, commercial ports have been vital to a state and disruption of their services can cause damage. For this reason, commercial ports are considered CIs. As ports are the blood veins of global economy and cross-border trade, there exists a network of interconnected CIs that have "physical and cyber multi-inter-dependencies, interacting with all sectors of the economy; therefore, their malfunctioning or disruption will have cascading effects on several other infrastructures or cross-border services that depend on them" [7].

1.2.2 Ports as Critical Information Infrastructure

The advanced development of information systems, and the evolution and diffusion of broadband communication has led to a wide adoption of *information and communication technology (ICT)* by CIs [7]. These ICT systems are critical for the normal functioning of the CI, and are themselves a form of critical infrastructure. *Critical Information Infrastructure (CII)* are ICT systems that are CIs for themselves or that are essential for the operation of one [21]. Examples of ICT systems, which may also serve CIIs, include communications systems, as shown in Table 1.2.2.

Ports host CIIs, and their disruption would have significant consequences [22]. "The large amount of critical and sensitive data, the information and services that are managed daily, the number of entities called to be served, and the inter-dependencies with other infrastructures require effective security management" [7]. The malfunctioning or disruption of a single CII that is connected to a network could effect an entire network of users (CIs) and the services that depend on them. The drawback of making ICTs the backbone of CIs is that it leaves systems vulnerable to exploitation or manipulation from threats [23].

Table 1.2 *Many ICT systems can be found in a port, some examples are included in the table below.*

ICT Systems	**Examples**
Security	Vehicle access, building access, control gates
Communications	Mobile radio, email, websites for cargo and customs
Business	Terminal Operation System, Container Terminal Management System, office systems, e.g. payroll
Terminal automation	Vessel scheduling software, yard equipment and maintenance, control systems for cranes, Remote monitoring of equipment

Source: Boyes [24].

1.2.3 Impact of Port Disruption

Disruption refers to a disturbance in which material flows are stopped entirely, while *delay* refers to a disturbance in which the rate of material flows is slowed [25]. Both delay and disruption will postpone the time of arrival of goods, and are risks for ports [26]. For the purpose of this chapter, disruption and delay will be referred to simply as "disruption." Some scenarios that cause port disruption include natural disasters, labour strikes, climate change and cyber-attacks.

Port disruption has a domino effect, posing both costs and benefits to other ports. It is worth noting that ports compete for cargo, and there could be much to gain from a well-timed disruption at a neighboring port. For instance, a five-day shutdown of a US West Coast port would result in ships being re-routed to East Coast ports. To reach the US East Coast, these ships- most too large to cross the Panama Canal- would transverse the Suez Canal and this would delay their shipment by almost a week [27]. In this scenario, US East Coast ports benefit by gaining shipments and the Suez Canal suffers due to unexpected congestion. The degree of coordination that goes into the flow of cargo highlights the inter-dependency of ports and means the impact of disruption is widely felt. This Subsection explores five potential hazards of port disruption: congestion, economy, environment, geopolitics and safety.

1.2.3.1 Congestion

Port activity is increasingly required to fit perfectly into wider logistics chains, but congestion can prevent a match between ports and their network. When a port suffers *congestion*, it is understood that ships are queuing, waiting to obtain a berth [28]. The busier the traffic, the greater the imposed cost [29]. Congestion costs include time loss, additional fuel consumption, inconvenience and possibly even accidents [29]. However, time loss is the largest contributing factor, and this is transferred to others. According to Hapag Lloyd, a shipping company, their liners often call at over a dozen ports per voyage [30]. Delays can impact operations and congestion may be felt elsewhere in the logistics chain.

1.2.3.2 Economy

Ports are major economic multiplier for a state's prosperity [9]. In 2018, nearly 80 per cent of the world's trade volume and 70 per cent of its trade value passed through ports [31]. Ports are vital to trade and their disruption, in addition to the effect on port operations, would cause damage to trade flows, economies and various parties concerned [25, 7]. The economy is a concern for many stakeholders ranging from states to the firms and people affected by maritime business around the globe [25]. Ironically, ports and shipping are among the most important causes for uncertainty in supply chains [32].

1.2.3.3 Environment

Environmental pollution is another potential hazard of port disruption. Oil and gas tankers compose one of the highest risks in a port environment, with the majority of such accidents involving tanker vessels, barges, platforms and petroleum shore stations [33]. Further, some pollution areas are caused by illegal human activities such as tanker cleaning. Every year, diesel, oil, petrol and other toxic chemicals are released into the sea, causing damage to wildlife, habitats, and ecosystems. While illegal dumping is not always accidental, such accidents could have catastrophic affects on the environment. Minimizing the opportunity for accidents means actively working to ensure security of ports and ships, including the cybersecurity of their physical systems which may, if vulnerable, be leveraged by adversaries. To minimize the possible damage to the environment, it is essential to develop and implement robust cybersecurity measures.

1.2.3.4 Geopolitics

Protection of critical infrastructure has always been at the center of homeland security. After all, if you don't have food, water, energy, power, and communication, you don't have a country [34]. As critical infrastructure, ports are important to a state both strategically and politically. The value of a port to the economy of a country has been demonstrated in war time: "Ports are a primary object in each campaign, for the enemy knows well the crippling effect on his opponent of capturing, or even putting out of action, the ports through which supplies, arms and men reach the fighting zone" [3]. Port disruption represents a geopolitical hazard for states by compromising their capabilities.

1.2.3.5 Safety

Ports are dangerous places to work for both dockworkers and seafarers, who undergo extensive safety training to minimize workplace accidents. Maritime safety has many influencing human factors, including fatigue, stress, teamwork, communication, and safety culture [35]. Port disruption can effect these factors, sometimes interfering with basic services like communication, to increase the safety risks to people [7]. Further, the disruption of CIIs could impact safety [22]. Also, serious accidents themselves can disrupt ports, and are detrimental to port growth and efficiency, not to mention its reputation [25].

1.3 Cybersecurity

Cybersecurity is "the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse" [36]. This includes intentional harm by a system operator or accidental harm as a result of failing to follow security procedures.

Mission-critical information assets, an organisation's 'crown jewels,' are of great value and would cause a major business impact if compromised. Cybersecurity measures need to protect these crown jewels against a range of low-level crime to national security concerns. This is accomplished through an understanding of the vulnerabilities and threats to business. This Section analyses fundamental cybersecurity properties of information systems in Subsection 1.3.1, that are essential in preventing exploitation of vulnerabilities by threats in Subsection 1.3.2 which lead to cyber-attacks in the maritime sector which are defined in Subsection 1.3.3.

1.3.1 Cybersecurity Attributes

Desirable characteristics of a secure system have come to be defined by the *CIA triad* [37], which includes three core cybersecurity attributes: confidentiality, integrity and availability. *Confidentiality* focuses on control and authorisation of information access and disclosure, with respect to privacy. A critical cybersecurity concept is the *principle of least privilege*, whereby access to information and assets should be granted only on a need-to-know basis. *Integrity* protects against improper information modification or destruction and maintains consistency, accuracy, and trustworthiness of data or system. *Availability* ensures timely and reliable accessibility and use of data, asset information, systems, and associated processes.

The CIA triad is the heart of information assurance standards and guides policy for information security in an organization. Organizations should have management, operational and technical security controls in place to protect the confidentiality, integrity, and availability of their systems and information.

Further, effective and holistic cybersecurity requires information systems to be built on four pillars: people, processes, technology and physical aspects [38]. Ultimately, when combined into a single, integrated framework, this holistic strategy will yield the most effective cyber defenses in ports.

1.3.2 Vulnerabilities and threats

The exponential growth of the internet and interconnected devices has created manifold benefits for society and the economy, but with these benefits come new cyber vulnerabilities and threats.

A *vulnerability* is a weakness in an information system, its security procedures, internal controls, or implementation that could be exploited by a threat [39]. Many common vulnerabilities relate to hardware, software, networks, personnel and organizations [40]. Most information system vulnerabilities are associated with security controls that either have not been applied (intentionally or unintentionally), or have been applied, but retain some weakness [41]. Organizations may need to reassess existing security controls over time to determine effectiveness of their controls.

A *threat*, on the other hand, is a circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the nation through unauthorized access, destruction, disclosure, modification, or denial of service to an information system [39]. Threats can be intentional, accidental, untargeted or targeted in nature, as seen in Table 1.3.2.

A situation or event caused by a threat that has the potential for adverse impact is referred to as a *threat event* [39]. When a threat event occurs, it becomes an incident that can jeopardize the confidentiality, integrity, or availability of an information system or constitute a violation of security policies, procedures, or their use [44].

The level of *impact* from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure, modification, destruction, or loss of information or loss of information system availability [45]. Organizations can experience the impact of adverse events at the information system level (e.g., failing to perform as required), at the business level (e.g., failing to meet business objectives), and at the organizational level (e.g., failing to comply with legal or regulatory requirements, damaging reputation or relationships) [41].

A cybersecurity threat is actualized by a *threat actor*, who is a person or entity responsible for an incident and can be internal or external to an organization [46]. Threat actors have a variety of motivations and capabilities which require the use of different risk mitigation and control techniques [39]. Some actors are motivated by financial gain, while others are motivated by political, ideological or religious reasons. Threat actors include hacktivists, criminals, disgruntled insiders and states.

Organizations often categorize the *tactics, techniques* and *procedures (TTPs)* of adversaries to create *threat scenarios* that describe how a threat can orchestrate and impact their business. For adversarial threats, an assessment of likelihood of

Table 1.3 Categorization of common cyber-attacks in the maritime industry based on two factors: (1) threat sources intent and (2) target.

	Intentional	**Unintentional**
Targeted	Brute force Denial of service Spear-phishing	Victim to social engineering Escaped proof-of-concept Runaway penetration test
Untargeted	Malware Phishing Water holing Scanning	User error

*Source:*Bimco (2017), CERT-UK (2015) [42, 43]

Table 1.4 The common threat actors groups in the maritime industry, their motivations, the groups they exist within and their targets.

Threat Actor Groups	Motivations	Threat Actors	Targets
Criminals	Economic/ Financial Information advantage Reputation	Individuals Organizations	Assets Individuals Organizations
Espionage	Commercial/ Industrial Intellectual property Competition	Organizations Nations	Governments Individuals Organizations
Hacktivists	Challenge/ Egoism Ideological/ Political/ Social change	Activists Individuals	Governments Individuals Organizations
Insider threats	Financial gain Revenge	Contractors Employees Partners	Physical/ Process/ Technical failures Poor operational design
Terrorists/ War[1]	Political/ Social change Fear Religion/ Ideology	Hackers Individuals Terrorists States	Individuals Infrastructures Organizations Public/ Critical targets Governments/ Military

[1] The authors have combined the categories cyber-terrorist and cyber-war.
Source: Boyes [47].

occurrence and the success of an attack is typically based on the adversary's intent, capability and targeting [39, 41]. Table 1.3.2 analyses the main threat actor groups, their motivations, the groups they exist within, and their targets.

1.3.3 Cyber-Attacks

Of the many challenges facing the modern port, one of the most complex and potentially damaging is the threat of a large-scale cyber-attack against information communication technology and cyber infrastructure.

Cyber-attacks include nefarious activities that target both *Information Technology (IT)* systems, or cyber assets, and *Operational Technology (OT)* systems, or physical assets, computer networks, or personal computer devices in an attempt to compromise, destroy or access systems and data [45]. Breaches result in property damage or theft, data damage, loss of income due to outages and operational failure, website defacement, and cyber extortion. The consequences of a cyber-attack depend on the nature of the attack, incident complexity and established industry procedures.

An *attacker* is a party who attacks a host, network, or other IT resources [44]. Not all attacks are intentional, as some result from users who accidentally or unintentionally violate security policies or requirements, to the point of compromising security, as seen in Table 1.3.2. Attackers who intend to exploit vulnerabilities are motivated by various reasons, ranging from the desire to make political or social statements to financial gain and cyber warfare. The skill sets of attackers vary widely as do their motivations. Attackers commonly violate cybersecurity attributes in the CIA triad: confidentiality, integrity, and availability.

Attackers utilise paths to gain access to a target, known as *attack vectors* [48]. Each attack vector can be thought of as comprising a source of malicious content, a potentially vulnerable processor of that malicious content, and the nature of the malicious content itself. An example of a threat vector is a malicious email attachment (content) in an email client (source) rendered by a vulnerable application (processor). The section below explores common attacks vectors found in ports, which have led to significant breaches in recent years, as discussed further in Section 1.5.

Advanced Persistent Threat (APT)

This attack is widely acknowledged to be the most sophisticated and potent class of security threat. APTs are specifically designed to quietly, slowly spread to other hosts, gathering information over prolonged periods of time and eventually leading to exfiltration of sensitive data and cause other negative impacts [49]. The threat actors involved are technological experts who are well-trained, well-funded, organized, and capable of utilizing a range of technologies to achieve their objectives.

Backdoor

A *backdoor* is an undocumented way of bypassing normal authentication procedures that enables remote access to a system [45]. Although some backdoors are secretly installed, others are deliberate and widely known. These backdoors were originally designed to provide the manufacturer with a way to restore user passwords.

Malware

Malware, or malicious software, is designed to gain access or cause damage to a computer, server or network without the knowledge of the victim [45]. Malware steals resources from a computer and exploits known deficiencies and problems of the network such as outdated or unpatched software. Examples of malware include viruses, Trojan horses, ransomware, spyware and worms. According to the *2018 Maritime Cyber Security Survey* by IHS Markit and BIMCO, 77 per cent of cyberattacks in the maritime industry are malware attacks [50].

Phishing

Sending e-mails to a number of potential targets asking for particular pieces of sensitive information, *phishing*, is a social engineering technique designed to deceive the user into disclosing sensitive or confidential information [45]. *Spear-phishing*, on the other hand, targets specific individuals with personalized e-mails containing malicious software or links.

Ransomware
Ransomware is a type of malware that locks a computer, holding it "hostage" by means of file encryption, forcing victims to pay money in order to get their files back [51]. Ransomware has become a lucrative business with increasing popularity.

Social engineering
Social engineering is a non-technical practice used to manipulate individuals within an organization into breaking security procedures [45]. There are many social engineering tactics and mediums of implementation, such as email, web, phone or USB drives. Phishing is an example of social engineering.

Virus
A *virus* is a computer program that can self-replicate and infect a computer without permission or knowledge of the user [45]. A virus might corrupt or delete data on a computer, spread to other computers by attaching itself to an active host program or an already-infected program and execute code when a user launches these programs.

Worms
A computer *worm* makes as many possible copies of itself from computer to computer [45]. It can self-replicate without any human interaction and does not need to attach itself to a program in order to cause damage. Worms can modify and delete files and even inject additional malware into the computer. In contrast to viruses, which require an already-infected host file to propagate, worms are standalone malware and do not require a host program or a human to spread.

To protect users from being victimized by the above attacks, protective approaches are needed not only to detect these malicious programs, but also to prevent them from inflicting damage and compromising the CIA triad in the first place. To do so, a profound understanding of the nature of attacks is required for in-depth examination of vulnerabilities to develop effective defensive solutions.

1.4 Ports and Cybersecurity

Unlike the sea and port, cyberspace is not a geographical domain [1]. However, physical and cyber domains not only affect each other, but interact and intersect to create a unique cyber-physical domain. Adopting cybersecurity attributes provides a modern framework to facilitate collaboration between security and safety specialists. When applying these attributes to cyber-physical systems, we gain insight into cyber-vulnerabilities. This Section explores ports as a cyber-physical environment in Subsection 1.4.1 and the cybersecurity attributes specific to ports in Subsection 1.4.2.

1.4.1 Port as a Cyber-Physical Environment

A *cyber-physical system (CPS)* is an "integration of computation with physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa" [52]. CPSs are systems of collaborating computational entities which link the surrounding physical and virtual to achieve a global behaviour [53]. CPSs are composed of a set of networked agents interacting with the physical world; these agents include sensors, actuators, control processing units, and communication devices that enable automation [54, 55]. These sectors control Industrial Control Systems (ICSs) through the use of SCADA systems, Distributed Control System (DCS) and IoT, which are based on the nature of individual systems [56].

The global supply chain is a complex CPS composed of distinct, interconnected *Information Technology* (IT) and *Operational Technology* (OT) systems [7]. The difference is that IT manages the flow of digital information, while OT deals with machines and physical processes [57]. A traditional juxtaposition would be that of software (IT) vs. hardware (OT) [57]. However, this does not stress the interaction of cyber and physical elements. It is not sufficient to understand IT and OT components separately. Rather, CPS is about the intersection of physical and cyber [52].

The fundamental ICT systems of ports simplify and accelerate processes, and form a foundation for an Intelligent Transport System (ITS) [58]. Ports use ICT systems to manage, store and share information, ensuring swift and seamless product/ data exchange from the producer to end consumer during the provision of services [7]. Ports use a wide array of ICT systems to perform vital functions, including communications, security, business, and terminal automation, as seen in Table 1.2.2.

As the cyber-physical environment grows in ports, so does vulnerability. The smartening of ports does not necessarily increase threats (the number, capability, or intent of threat actors), but it does increase vulnerabilities (in the form of a larger and more complex attack surface) and it increases the potential consequences (by allowing attacks on networks and data to cause physical damage in the real world) [59].

Likewise, it is key to acknowledge the "the three sides of the coin:" Ship, shore and their connections [60]. As ports and ships become smarter, their communication and information-sharing efforts grow in sophistication. The harmonized collection, integration, exchange, presentation and analysis of marine information on board and ashore by electronic means can be referred to as *e-Navigation* [60]. Ship-borne users of e-Navigation include off-shore energy vessels, fishing vessels and commercial tourism craft; shore-borne users encompass ship owners and operators, port authorities, insurance and financial organizations. For instance, congestion may lead to port disruption, but e-Navigation may help reducing delays by means of modulating a ship's journey. While e-Navigation increases efficiency in ports and works to protect the marine environment, it also raises cyber-risks from the susceptibility of port systems to cyber-attacks.

1.4.2 Cybersecurity Attributes of Ports

The CIA triad alone is not adequate to manage infrastructure susceptibilities. The *Parkerian Hexad* provides a fortified approach to encompass both information insurance and engineering good practice [61]. This model includes the three CIA attributes, and three additional attributes: authenticity, utility and possession/ control. Further, a extended version of the Parkerian Hexad, by Boyes, includes two additional attributes: safety and resilience. These eight attributes demonstrate a comprehensive cybersecurity model for ports [38], shown in Table 1.4.2.

In this model, the attributes from Table 1.4.2 address four distinct operations, whereby controlled access to port systems falls under the first two attributes: (1) confidentiality, and (2) possession/ control. Port system configuration, information quality and validity, are included in the next three attributes: (3) integrity, (4) utility, and (5) authenticity. Finally, the continuity of port operations, safety of people and assets are encompassed by the last three attributes: (6) safety, (7) resilience, and (8) availability. These four operations are shown in Figure 1.1.

Table 1.5 This table shows the eight maritime cybersecurity attributes by Boyes. It is a extended version of the CIA Attributes and the Parkerian Hexad, and includes two additional attributes: safety and resilience.

Attributes	Definition
Confidentiality	The control and authorisation of information access and disclosure, with respect to privacy. [1] Systems should prevent unauthorised access to sensitive data and personal data should be handled in accordance with the General Data Protection Regulation (GDPR).[2]
Possession/ control	Systems shall be designed, implemented, operated and maintained so as to prevent unauthorised control, manipulation or interference.
Integrity	Protect against improper information modification or destruction and maintain consistency, accuracy, and trustworthiness of data or system.[12]
Utility	Ensure asset information and systems remain usable and useful across the life-cycle of the asset.
Authenticity	Ensure system inputs and outputs, the state of any associated processes and data, are genuine and have not been tampered with or modified.
Safety	The design, implementation, operation and maintenance of systems and related processes to prevent harmful states that may lead to injury, loss of life, unintentional physical or environmental damage.[3]
Resilience	The ability of the asset information and systems to transform, renew and recover in a timely way in response to adverse events.[3]
Availability	Ensure timely and reliable accessibility and use of data, asset information, systems, and associated processes.[12]

[1] Dukes, CW [37]
[2] Parker, Donn B. [61]
[3] Boyes, H., Isbell, R. and Luck, A. [38]
Source: Boyes [62]

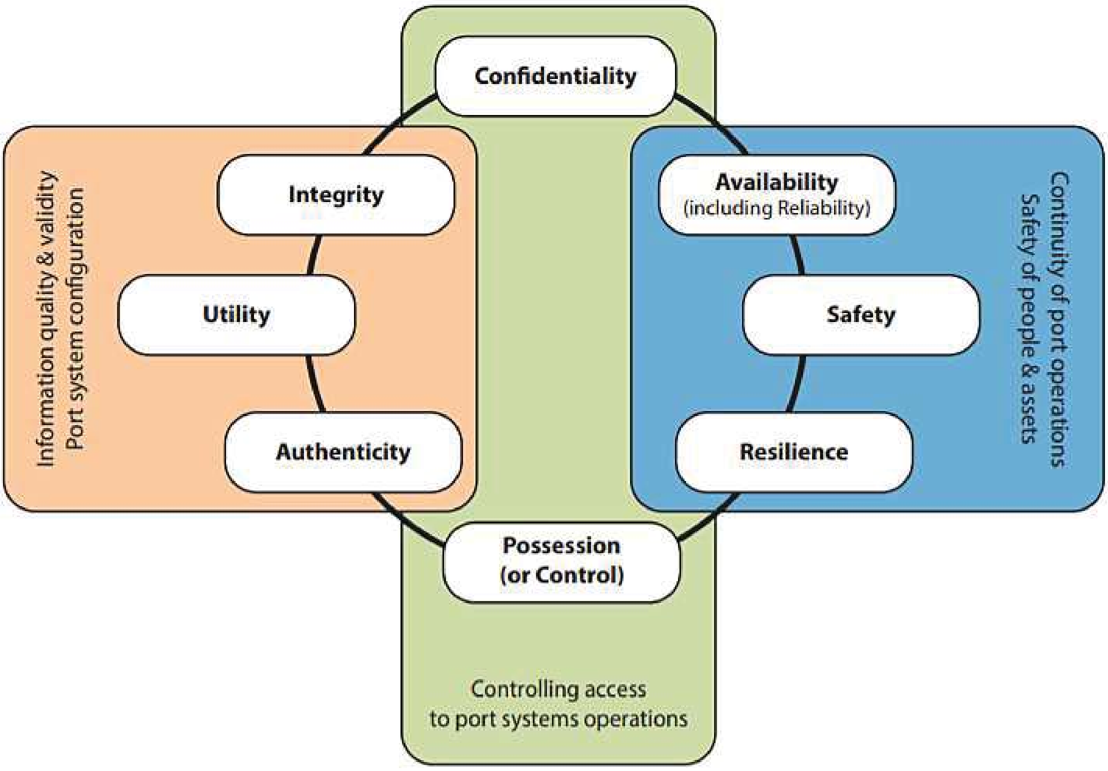
Confidentiality
Integrity
Utility
Authenticity
Availability
(including Reliability)
Safety
Resilience
Possession
(or Control)
Information quality & validity
Port system configuration
Continuity of port operations
Safety of people & assets
Controlling access
to port systems operations

Figure 1.1 This table shows the four operations addressed by the eight maritime cybersecurity attributes by Boyes.

1.5 Attack Scenarios

There are many known cyber attacks in maritime ports, however only a fraction of the attacks which occur are public knowledge. “Criminal organizations have hacked the computers and networks of shipping lines and their agents, port authorities, and port operators to obtain information on ship-sailing schedules, ports of call, the specific cargoes and containers on-board, load/ manifest data, trucker information, cargo release information in destination ports, and which security measures are in place” [63]. The 2018 Maritime Cyber Security Survey [50] reveals that phishing (49 per cent) and malware (44 per cent) were the most common form of incidents faced by in the maritime sector, mostly leading to service disruption (49 per cent) and system downtime (44 per cent). This section investigates common attack vectors that have been observed in the ports and provides five real cyber-attack scenarios, summarized in Table 1.5, to illustrate the cyber-threat landscape.

1.5.1 APT40

APT40’ is a cyber-espionage threat actor group believed to be sponsored by the Chinese state that has been targeting engineering, transportation and defence industries that overlap with maritime technologies. The earliest public reports from Proofpoint show a pattern of sending targeted emails, or spear phishing, to a number of US

Table 1.6 Cyber Attacks

Year[1]	Attack Scenario	Threat Actor	Attack Type
2019	APT40	Cyber-espionage	Phishing Backdoors Web server exploitation Web compromise
2018	The Port of San Diego	Criminals	Ransomware (Malware)
2017	Maersk NotPetya Attack	Terrorists/ War	Worm (Malware)
2014	Danish Port Authority	Terrorists/ War	Phishing Backdoors Virus
2013	The Port of Antwerp	Criminals	Phishing

[1] Year attack was discovered

shipbuilding companies and organisations with maritime links, which if successful would have resulted in backdoor software being installed on the target machine. The actor then used this access to move laterally within the organisation and use information gleaned (e.g. account credentials) to help them target other organisations. FireEye reports that they expect this group's activities to continue in at least the near and medium term despite the recent public attention [64].

1.5.2 The Port of San Diego

In 2018, five days after an attack on the Port of Barcelona [65], the Port of San Diego's IT systems were disrupted by ransomware (malware) that prompted investigations by the Federal Bureau of Investigation and the Department of Homeland Security [66]. Once inside the victim's network, the attacker used the program to encrypt valuable data, then demand a ransom payment in Bitcoin in exchange for the decryption key [67]. The threat actor group allegedly attacked more than 200 targets, including hospitals, health care companies and public institutions, with the Port of San Diego being their most recent victim [67]. The indictment alleges that two cyber-criminals have collected over six million dollars in ransom payments to date, however the port did not pay the ransom demand. The attack took down non-critical administrative systems for a brief period, and did not affect commercial port operations. According to the Port of San Diego, no data loss occurred as a result of the attack because the port's IT team had backups in place [67].

1.5.3 Maersk NotPetya Attack

The Maersk NotPetya Attack took its name from its resemblance to *Petya*, a ransomware which surfaced in 2016, used to extort victims to pay for a key to unlock their files [68]. However, the ransom messages of NotPetya were only a ruse: the goal was purely destructive. The attack included a worm (malware) that would irreversibly encrypted computers' master boot records, the part of a machine that tells it where to find its own operating system. Any ransom payment that victims tried to make was futile: no key existed to reorder the contents of their computer.

The attack, which originated in Ukraine and has been attributed to a threat actor group tied the Russian state [69], was likely more explosive than its creators intended [68]. It cost AP Moller-Maersk, which was not even the intended target of the attack, at least USD 300 million [69]. It even spread back to Russia, striking the state oil company Rosneft [68]. "But the story of NotPetya isn't truly about Maersk, or even about Ukraine. It's the story of a nation-state's weapon of war released in a medium where national borders have no meaning, and where collateral damage travels via a cruel and unexpected logic: where an attack aimed at Ukraine strikes Maersk, and an attack on Maersk strikes everywhere at once" [68]. The release of NotPetya was an act of cyberwar, and has been included in the terrorists/ war threat actor group in Table 1.5.

1.5.4 Danish Maritime Authority

In April 2012, the Danish Maritime Authority was subjected to a cyber-attack. The phishing attack was carried out when a Danish Maritime Authority employee's computer was infiltrated by an email with an infected PDF attachment containing a virus [70]. When the employee opened the infected PDF file, hackers were given back-door access to the contents of his computer and the rest of the Maritime Authority's network. The virus spread through the port network and successfully reached other Danish government institutions [71]. The attackers stole sensitive information from Danish shipping companies and the merchant navy [70].

The Danish authorities eventually discovered the attack two years later and stopped the infiltration by shutting down the entire system for several days before reopening it with new anti-virus programs to further prevent such attacks [70]. It was difficult to assign blame without the necessary evidence, but according to the Danish Defense Intelligent Service report, the attack was sponsored by another state [72] and thus is classified under the terrorists/war threat actor group in Table 1.5.

1.5.5 The Port of Antwerp

Over a two-year period, from 2011-2013 the Port of Antwerp suffered an attack, whereby the movement and location of containers was intercepted and controlled by drug traffickers, who were able to hide illegal drugs among legitimate cargo [73]. These attackers are included in the criminal threat actor group in Table 1.5.

The group sent malicious software via e-mail, by means of a *phishing attack*, to the staff, which enabled them to get remote access to the port's data [74]. Although this first attempt was identified and a firewall was installed to prevent further attack, the hackers managed to break into port facilities and fit key-logging devices on the legitimate computers [74]. In this way, they gained wireless access to keystrokes typed by staff and captured screenshots from their computers [74]. When containers began to vanish entirely, the attack became apparent to the Port of Antwerp and they went to official authorities to ”uncover the mystery of the missing cargo” [73]. The drug smuggling operation was discovered and over 1000kg of cocaine and heroin seized [64]. To prevent further such attacks, the Port of Antwerp installed a firewall, but it is worth mentioning that the hackers were able to breach that remotely. [73].

This was one of the earliest cyber attacks in the maritime industry to be made public, being disclosed by Europol in 2013 [64]. It illustrates how cyberspace is another realm in which traditional crimes can be committed. It also highlights the intertwinement of cyber and physical systems [73].

1.6 Cyber Risk Management for Ports

A 2018 survey by the Global Maritime Forum on issues in the maritime industry ranked cyber-attacks and data theft as the highest in likelihood, third highest in impact, and lowest in industry preparedness [75]. *Cyber risk*, or information security risk, arises from loss of confidentiality, integrity, or availability of information or information systems and reflect potential adverse effects to organizational operations (i.e., mission, functions, image, or reputation), assets, individuals, other organizations, and the state [39]. This Section explores risk assessment in Subsection1.6.1, risk management in Subsection1.6.2, and risk strategy for ports in Subsection1.6.3.

1.6.1 Risk Assessment

Allianz’s 2019 Risk Barometer [2] classified cybersecurity as the most feared trigger of business interruption. A *risk* identifies the conditions under which external or internal threats can exploit existing vulnerabilities to cause an incident and damage assets [76]. Also called Cybersecurity Assessment (CSA), *Cyber Risk Assessment* is the process of identifying, estimating, and prioritizing information security risks [39]. The ISO/IEC 27001:2013 provides a consolidated standard framework for information security management, and says risk assessment is characterized by three risk activities, outlined in Table 1.6.1: identification, analysis and evaluation [77]

The complexity of infrastructure, paired with rapidly evolving security and safety requirements, makes it essential to have a proactive, comprehensive and integral approach to identifying risk in the ICT and physical system of ports [78]. *Risk Identification* is the process of recognizing and describing risks [77]. Once the risks are identified, they are classified according to likelihood and impact. *Risk Analysis* includes a review of identified risks to provide a quantitative estimate for the likelihood of a specific risk and the related impact on assets [77]. During *risk evaluation*, each risk is compared against an evaluation criteria, where risks are measured against security requirements indicating the required security measures’ [79, 77]. This is

Table 1.7 ISO 27001:2013 provides a standard framework for information security management, where risk assessment is characterized by three activities: identification, analysis and evaluation.

Risk Assessment	Definition
Identification	Recognize and describe risks.
Analysis	Review identified risks, estimate the likelihood and impact.
Evaluation	Compare each risk against an evaluation criteria.

Source: ISO [77].

where it is decided how risks will be treated. Steps will then be taken to exploit opportunities, counter threats and protect the global supply chain [80].

1.6.2 Risk Management

Risk management aims to protect business assets (physical and cyber) and minimize costs in case of failures. Risk management is based on the experience and knowledge of best practice methods, which consist of an estimation of the risk situation based on the business process models and organizational infrastructure. “These models support the identification of potential risks and the development of appropriate protective measures” [7].

Cyber risk management consists of the process of identifying, analysing, assessing, and communicating a cyber risk. It also includes accepting, avoiding, transferring, or mitigating cyber risk to a desired level. It takes into consideration the costs and advantages of actions taken by stakeholders. It aims to support safe and secure shipping that is operationally resilient to cyber risks, and it extends from senior management level to all operators in the port facilities [7]. In light of increasing risk, the International Maritime Organization (IMO) issued high-level guidelines on maritime cyber risk management in 2017 to support safe and secure shipping from current and emerging cyber threats. These guidelines present five functional elements of effective cyber risk management: identify, protect, detect, respond, and recover’ [81].

The maritime industry significantly focuses on the security and risk management of physical security [7]. However, the emerging landscape of IT-empowered CII-based critical infrastructures requires a shift in how the industry thinks about risk assessment [82]. When cyber risk management is effective, it considers safety and security effects consequent to the revelation or exploitation of vulnerabilities in information technology systems. Cyber risk management should be durable and evolve as a natural extension of already existing practices and strategies of safety and security management [60].

1.6.2.1 Coordinated Risk Management

Collaboration is prudent to "achieve better validation of the source of critical elements of software and hardware, particularly for systems that contain high value, sensitive information" [80]. Most existing risk management methodologies tend to focus too much on aspects of physical security and pay limited attention to CIIs, ignoring the complex nature of IT systems and assets used in the maritime sector, along with their interrelationships [82]. In order to reduce potential attack avenues, ports must have robust monitoring of and proper coordination between agencies [80]. A holistic method for managing security risks can help ports to check their compliance with existing legal, regulatory and standardization regime to detect possible violations, gaps, and a need for new regulations and directives [78].

1.6.3 Risk Strategy for Ports

As port and port operators are scattered around the globe, it is difficult to develop an overall strategy for all members of the port network. For example, the offices of a big container shipping line can be spread across 150 countries and the shipping line may operate 300 vessels [20]. This Subsection examines cyber insurance, investment decisions, and reporting.

1.6.3.1 Cyber Insurance

The cyber insurance market is emerging but may be considered relatively immature [83]. How to set premiums is a key question for the development of a more mature cyber insurance market. Setting premiums is particularly challenging for cyber risk, as there is limited information sharing regarding cyber incidents, leading to a lack of actuarial data from past events and lack of normative standards [84]. The ability to model cyber risk is currently limited but will improve substantially as more data is accumulated and shared [83]. Other cyber insurance challenges include a lack of legal framework, with uncertainty in liability and lack of cyber standards.

As new technologies are implemented and reliance on them grows, cyber risks are increasing and so is cyber-related loss [83]. Thus, it is likely that full cybersecurity for transportation infrastructure is not achievable solely through technological improvements [83]. Therefore, in addition to attempting to prevent attacks and reduce cyber risk, transportation managers should also prepare financially for inevitable losses through self-insurance and insurance [84]. Cyber insurance is currently available, but limited, and expansion of cyber insurance coverage is needed to manage risk [83].

1.6.3.2 Investment Decisions

Port terminals are both privately and publicly held, most often through leases that last anywhere from 25 to 50 years. To invest in automating a terminal, a process which takes about 10 years, a shipping company must be sure they will get a return on their investment before their lease expires. If there exists a large enough threat to this profit margin by means of cyber-attacks which could shut down business communications, disable physical security systems, and more, then port operators may reconsider leasing ports.

1.6.3.3 Reporting

An issue regarding cybersecurity awareness is the tendency of exploited organizations to refrain from reporting cyber attacks due to fear of damage to their reputation [85]. This has made the government responsible for making sure cyber attacks are reported. Today, it is often the case that national strategies are installed to legally require data breaches to be reported, and when they are not there are penalties- often in the form of fines. Some examples dictating these terms are the GDRPB [86] and EU Directive 2016/1148 [87]. This are explored further in Section 1.7.2.

1.7 Cybersecurity Guidelines and Standards

Over the past decade, governments, organizations and individuals have developed many strategies to strengthen cybersecurity in ports. Cybersecurity guidelines provide a framework for the risk assessment process whereby threats and vulnerabilities are identified to determine the risks they pose and establish an effective treatment plan [7]. The International Chamber of Commerce [88] categorizes these instruments into five groups: guidelines, national strategies, frameworks, standards of practice, and technical standards. These documents are summarized in Table 1.7. This section examines each group and gives authoritative examples of recommended practice in the maritime sector.

Table 1.8 Definitions and examples of high-level cybersecurity documentation in the maritime sector.

Documentation[1]	**Definition**	**Example**
Guidelines	High-level vision statements.	IMO Shipping Regulations
National Strategies	Articulate cybersecurity approach in national or legal context.	EU Directives and GDPR
Frameworks	Prioritize or evaluate resources that help benchmark progress.	NIST Cybersecurity Framework
Standards of Practice	Defines measures to enhance the security of port facilities and ships.	ISPS Code, ISO/IEC 27001 and Common Criteria

[1] Technical standards not included

1.7.1 Guidelines

Guidelines are high-level recommendations that scope concern for cybersecurity and provide a charter for individuals, organizations and states [88]. There exists multiple maritime industry cyber security best practice guidelines from organisations such as IET [38], IMO [89] and IALA [90]. This section will analyse the International Maritime Organization (IMO) regulations for shipping.

1.7.1.1 IMO Shipping Regulations

The *International Maritime Organisation (IMO)* is a specialized UN agency and is the primary regulator for shipping bodies [89]. In 2016, the IMO published guidelines for maritime cybersecurity management to provide high-level guidance related to the development and implementation of cyber risk management to safeguard the maritime sector from cyber threats [7].

In 2017, the IMO Facilitation Committee (FAL) and the Maritime Security Committee (MSC) issued guidelines for maritime cyber risk management in *MSC-FAL.1/Circ.3* [89]. With regards to ports, these guidelines place an obligation on shipowners, operators, and stakeholders to adopt a risk management approach to the financial consequences of a full or partial loss of availability, integrity and confidentiality of sensitive data .

Additionally, the 2017 *Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems* [91] encouraged administrations to formalise cybersecurity requirements in existing safety management systems (as defined in the ISM Code) no later than January 2021. These guidelines form the foundation of high-level statements across the maritime sector. It is worth noting that the IMO has yet to develop formal cybersecurity regulations specific to the maritime sector.

1.7.2 National Strategies

National strategies articulate an approach to cybersecurity tailored to a specific national or legal context [88]. These high-level documents are often based on guideline, which means that since the IMO has yet to develop cybersecurity regulations specific to the maritime sector, national authorities by-and-large have yet to do this as well [92]. This section describes national strategies in ports, namely, the EU Directives concerning cybersecurity and General Data Protection Regulation.

1.7.2.1 EU Directives and GDPR

In July 2016, the *EU Directive 2016/1148 (NIS Directive)* proposed a wide-ranging set of measures to boost the level of cybersecurity of network and information systems to secure services vital to the EU economy and society [87]. With respect to port facilities and ports, this Directive states that EU countries must take actions to improve cybersecurity capabilities that cover all operations, including radio and telecommunication systems, computer systems and networks. It also ensures maritime operators to take into account international codes and cybersecurity recommendations developed, especially IMO guidelines. Similarly, there are punishments applied by the state when these laws are not followed.

The 2018 *General Data Protection Regulation (GDPR)*, also known as *Regulation (EU) 2016/679*, requires all industries including the maritime industry to process personal data relating to EU data subjects, residents or citizens securely using appropriate technical and organisational measures [86]. With the adoption of the GDPR, organizations across the EU are required to report data breaches to the Information Commissioner's Office which promotes security and accountability. A violation of GDPR provisions attracts penalties of up to 20 million euros, or in the case of an undertaking, 4% of the organization's annual turnover, whichever is higher.

Under the *EU Cybersecurity Act*, which was developed in 2019, the position of ENISA is strengthened with regards to cybersecurity matters for EU Member states as the act defines an EU-wide cybersecurity certification framework for ICT products, services and processes [93]. This framework will provide a comprehensive set of rules, technical requirements, standards and procedures in order to attest that ICT products and services can be trusted based on EU requirements.

The *European Maritime Single Window (Regulation 2019/1239)* [94] ensures competitiveness, efficiency and environmental sustainability of the European maritime transport sector. It is necessary to reduce the administrative burden on ships and to facilitate the use of digital information and contribute to the integration of the sector to the digital multi-modal logistic chain. This is achieved through the submission of data elements required by both maritime and customs authorities using a harmonised cargo data set.

1.7.3 Frameworks

Developing national strategies further, *frameworks* gather a catalogue of prioritized or evaluated resources that help organizations to benchmark their maturity and progress in addressing cybersecurity risk [88]. An example of a framework that guides ports and port facilities is the NIST Cybersecurity Framework.

1.7.3.1 NIST Cybersecurity Framework

In 2018, The US National Institute of Standards and Technology (NIST) published a revised version of the 2014 framework for improving critical infrastructure cybersecurity, often referred to as the *NIST Cybersecurity Framework* [81]. Created through collaboration between industry and government, the voluntary framework consists of standards, guidelines, and practices to reduce cyber risks to critical infrastructure. As ports are critical infrastructures, the NIST framework can be applied as a prioritized, flexible, repeatable, and cost-effective approach to port cyber risk management. The NIST Core Functions, as seen in Table 1.7.3.1, allow organisations to view of the life-cycle of their management of cybersecurity risks [81].

1.7.4 Standards of Practice

Standards of practice are documents that guide or govern organizational processes to ensure robust and consistent operation of cybersecurity best practices [88]. This section describes well-known examples such as the ISPS code, ISO/IEC 27001 and Common Criteria.

Table 1.9 NIST Core Functions

NIST Core Functions	Definitions
Identify	Covers all personnel roles and responsibilities that need to be defined for cyber risk management and all systems, assets, data, and capabilities that when endangered can pose risks to the port and its ships.
Protect	Implementation of risk control processes and measures and the contingency planning to protect cyber activities and confirm the continuity of operations.
Detect	Development and implementation of all necessary activities that a port and its facilities need to detect a cyber-attack in time.
Respond	Activities that are needed to provide resilience and to restore systems necessary for operations and services.
Recover	Identification of measures that are necessary for back-up or restore of cyber systems for operations.

Source: NIST 2018 Framework [81].

1.7.4.1 The ISPS Code, ISO/IEC 27001 and Common Criteria

The *International Ship and Port Facility Security (ISPS) Code* was an amendment to the *Safety of Life at Sea (SOLAS) Convention* in 2002 and defines measures to enhance the security of port facilities and ships [95]. The aim of the ISPS Code is to enhance maritime security both on board ships and in ports. The traditional approach to maritime security was container security, however, the ISPS Code has recently included port cybersecurity with regards to access control and authentication requirements which will help the port authorities to secure their ICT systems and to better mitigate existing and upcoming cyber risks.

The ISPS Code has three security levels, ranging from low to high in proportion to the nature and scope of the incident or perceived security threat. The Code requires that ports and port authorities develop and implement improved *Port Facility Security Plans (PFSP)* for each operational level that outline the measures to be put in place to address threats and the countermeasures [95]. PFSP is based on the *Port Facility Security Assessment (PFSA)* and a risk-analysis scheme that is implemented by governments and authorized security organizations to identify major assets, possible threats and countermeasures.

The ISO/IEC 27000 family of standards [77] helps organizations keep information assets secure. The ISO/IEC 27001:2013 standard provides requirements for an information security management system (ISMS). The maritime industry implements this standard to:

- Examine the port's information security risks, taking account of the threats, vulnerabilities, and impacts.
- Design and implement information security controls and forms of risk treatment.
- Adopt an overarching management process to ensure information security controls continue to meet the port's information security needs on an ongoing basis.

Common Criteria, also known as ISO/IEC 15408 [96], is an international standard that provides independent, objective validation of the reliability, quality and trustworthiness of IT products. This demonstrates that manufacturers have met the necessary security requirements to sell their products in valuable markets, providing increased confidence. Common Criteria sets specific information assurance goals including strict levels of integrity, confidentiality and availability for systems and data, accountability at the individual level, and assurance that all goals are met.

1.8 Summary

The global port system is a mixed bag, where ports vary in structure and ownership. Each port, acting as a value multiplier in the system, is a critical infrastructure and includes critical ICT systems. The disruption of a single port could have a severe impact not only on port operations, but act as a domino effect across the system.

The interconnected networks of both information and cyber physical systems introduces new vulnerabilities and threats to ports, namely the threat of a large-scale cyber-attack on ICT systems and key infrastructure. It is imperative to act with urgency and purpose to protect the cyber domain from crippling attacks and disruption. Understanding ports as a cyber-physical environments allows us to classify cybersecurity attributes in ports, and manage cyber threats.

There are instances in which vulnerabilities are not well-managed, as presented in the five cyber-attack scenarios. These highlight the importance of cyber risk management in ports, and the need for a coordinated strategy. Existing guidelines and standards have strengthened cybersecurity in ports, but there is much work to be done. It is an uphill battle, as the proportion, complexity and evolving nature of cyber means there is no across-the-board way to respond to cyber-incidents.

This aim is further challenged by continuous evolution of the modern port, an increasingly faster pace at which mainstream technology is adopted. Amidst a technological revolution, the entire maritime industry is exploring, developing, and implementing new systems and innovative technology to achieve greater efficiency. Some technological trends shaping the port industry include autonomous ships, blockchain applications, cargo and vessel tracking [97]. But cyber and ports are not the only entities embracing the future. Just as ports evolve, and become smarter, so do cyber attackers. It remains a constant spar for the cutting edge, which in-turn propels the quest for the next wave of new technology and improved efficiency. While the future can only be predicted, it is certain ports and cyberspace are two realms that cannot again be separated.

References

[1] Ablon L, Binnendijk A, Hodgson Q, et al. Operationalizing Cyberspace as a Military Domain: Lessons for NATO. RAND Corporation; 2019. Available from: https://www.rand.org/pubs/perspectives/PE329.html.

[2] Allianz Risk Barometer. Allianz Global Corporate and Specialty SE; 2019. Available from: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Safety-Shipping-Review-2019.pdf.

[3] Oram R. Cargo Handling and the Modern Port. Pergamon; 1965.

[4] Fair M. Port administration in the United States. Cornell Maritime Press; 1954.

[5] Antunes C. Early modern ports: 1500 - 1750. Institute of European History; 2010. Available from: http://www.ieg-ego.eu/antunesc-2010-en.

[6] Christaller W, Baskin C. Die Zentralen Orte in Süddeutschland. Central Places in Southern Germany; Translated by Carlisle W. Baskin. Prentice-Hall; 1966.

[7] Polemi N. Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains. Elsevier; 2017.

[8] Hohenberg P, Lees L. The making of urban Europe, 1000-1994. Harvard University Press; 1995.

[9] Alderton P. Port Management and Operations. Informa. 2008;.

[10] Lloyd's List's One Hundred Container Ports 2018 Edition. Lloyds List Intelligence; 2018.

[11] Magnuson S. Security Around Signapore Critical to World Economy. National Defense Megazine. 2007;.

[12] Port Reform Toolkit: Second Edition. The International Bank for Reconstruction and Development / The World Bank; 2007. Module 3: Alternative Port Management Structure and Ownership Models.

[13] Monios J. Port governance in the UK: Planning without policy. Research in Transportation Business & Management. 2017 03;22:78–88.

[14] Yang Y, Zhong M, Yao H, et al. Internet of things for smart ports: Technologies and challenges. IEEE Instrumentation & Measurement Magazine. 2018 02;21:34–43.

[15] The history of the TEU (Twenty-foot Equivalent Unit); 2019. Available from: https://www.icontainers.com/us/2019/08/06/history-of-teu-twenty-foot-equivalent-unit/.

[16] Mega-Ships; 2019. Available from: https://www.joc.com/special-topics/mega-ships.

[17] Container Ship Design. World Shipping Council; 2019. Available from: http://www.worldshipping.org/about-the-industry/liner-ships/container-ship-design.

[18] Mega container ships and how they are changing ports. Ship Technology; 2016. Available from: https://www.ship-technology.com/features/featuremega-container-ships-and-how-they-are-changing-ports-4974826/.

[19] Habash R, Groza V, Burr K. Risk management framework for the power grid cyber-physical security. Current Journal of Applied Science and Technology. 2013;p. 1070–1085.

[20] Jensen L. Challenges in maritime cyber-resilience. Technology Innovation Management Review. 2015;5(4):35.

[21] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union; 2008.

[22] Alberts C, Dorofee A. OCTAVE Method Implementation Guide Version 2.0. Volume 2: Preliminary Activities. Carnegie Mellon University; 2001.

[23] Carrapico H, Barrinha A. The EU as a coherent (cyber) security actor? JCMS: Journal of Common Market Studies. 2017;55(6):1254–1272.

[24] Boyes H. Maritime Cyber Security–Securing the Digital Seaways. The Institution of Engineering and Technology. 2013;p. 56–63.

[25] Lam J, Su S. Disruption risks and mitigation strategies: an analysis of Asian ports. Maritime Policy & Management. 2015;42(5):415–435.

[26] Omer M, Mostashari A, Nilchiani R, et al. A framework for assessing resiliency of maritime transportation systems. Maritime Policy & Management. 2012;39(7):685–703.

[27] Cohen S. Economic Impact of a West Coast Dock Shutdown. 2019 10;.

[28] Jansson J, Shneerson D. Port Economics. vol. 8. MIT press; 1982.

[29] Meersman H, Van de Voorde E, Vanelslander T. Port congestion and implications to maritime logistics. In: Maritime Logistics: Contemporary Issues. Emerald Group Publishing Limited; 2012. p. 49–68.

[30] Hapag-Lloyd. Container ships soon to sail unmanned?; 2015. Available from: https://www.hapag-lloyd.com/en/news-insights/insights/2015/08/container-ships-soon-to-sail-unmanned_42532.html.

[31] Review of Maritime Transport 2018. United Nations Conference on Trade and Development (UNCTAD); 2018.

[32] Sanchez-Rodrigues V, Potter A, Naim M. Evaluating the causes of uncertainty in logistics operations. The International Journal of Logistics Management. 2010;21(1):45–64.

[33] Silgado D. Cyber-attacks: a digital threat reality affecting the maritime industry. World Maritime University Dissertations; 2018.

[34] Lewis T. Critical infrastructure protection in homeland security: defending a networked nation. New Jersey: John Wiley & Sons; 2014.

[35] Hetherington C, Flin R, Mearns K. Safety in shipping: The human element. Journal of safety research. 2006;37:401–11.

[36] National Cyber Security Strategy 2016-2021. UK Government; 2016. Available from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf.

[37] Dukes C. Committee on national security systems (CNSS) glossary. CNSSI, Fort Meade, MD, USA, Tech Rep. 2015;4009.

[38] Boyes IR H, Luck A. Good Practice Guide Cyber Security for Ports and Port Systems. Institution of Engineering and Technology. 2020;.

[39] Special Publication 800-30 Guide for conducting risk assessments. National Institute of Standards and Technology; 2012. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[40] ISO/IEC 27005:2018 — Information security risk management. International Organization for Standardization; 2018.

[41] Special Publication 800-39 Managing Information Security Risk: Organization, Mission, and Information System View. National Institute of Standards and Technology; 2011. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

[42] The Guidelines on Cyber Security Onboard Ships. BIMCO; 2017. Available from: https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=20.

[43] Common Cyber Attacks: Reducing The Impact. GHCQ & CERT-UK; 2015. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf.

[44] Stouffer K, Falco J, Scarfone K. Draft NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology; 2011. Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[45] CNSSI 4009 National Information Assurance (IA) Glossary. Committee on National Security Systems (CNSS); 2015.

[46] Bodeau D, McCollum C, Fox D. Cyber Threat Modeling: Survey, Assessment, and Representative Framework. HSSEDI, The Mitre Corporation; 2018.

[47] Boyes IR H, Luck A. Code of Practice: Cyber Security for Ports and Port Systems. Institution of Engineering and Technology. 2016;28.

[48] Souppaya M, Scarfone K. Special Publication 800-154 Guide to Data-centric System Threat Modeling. National Institute of Standards and Technology; 2016. Available from: https://csrc.nist.gov/csrc/media/publications/sp/800-154/draft/documents/sp800_154_draft.pdf.

[49] Cybersecurity Fundamentals Glossary. ISACA; 2016.

[50] Fairplay and BIMCO Maritime Cyber Survey 2018. Fairplay and BIMCO; 2018.

[51] NCSC glossary; 2016. Available from: https://www.ncsc.gov.uk/information/ncsc-glossary.

[52] Lee E, Seshia S. Introduction to embedded systems: A cyber-physical systems approach. Mit Press; 2016.

[53] Monostori L. In: Chatti S, Tolio T, editors. Cyber-Physical Systems. Berlin, Heidelberg: Springer Berlin Heidelberg; 2018. p. 1–8.

[54] Cardenas A. Cyber-Physical Systems Security Knowledge Area. The Cyber Security Body Of Knowledge. 2018;1.0.

[55] Brinkmann M, Hahn A. Testbed architecture for maritime cyber physical systems. In: 2017 IEEE 15th International Conference on Industrial Informatics (INDIN). IEEE; 2017. p. 923–928.

[56] Colbert E, Sullivan D, Kott A. Cyber-Physical War Gaming. Journal of Information Warfare. 2017;16(3):119–133.

[57] Coolfire. What Is The Difference Between IT And OT?; 2019.

[58] Fok E. An Introduction to Cybersecurity Issues in Modern Transportation Systems. ITE Journal. 2013;83(7):18–21.

[59] Habibzadeh H, Nussbaum B, F A, et al. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society. 2019;50:101660. Available from: http://www.sciencedirect.com/science/article/pii/S2210670718316883.

[60] Strategy for the Development and Implementation of E-Navigation. International Maritime Organization (IMO); 2019. Available from: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/eNavigation.aspx.

[61] Parker DB. Fighting Computer Crime: A New Framework for Protecting Information. New York, NY, USA: John Wiley & Sons, Inc.; 1998.

[62] Boyes H. Cybersecurity and cyber-resilient supply chains. Technology Innovation Management Review. 2015;5(4):28.

[63] Sen R. In: Cyber and Information Threats to Seaports and Ships; 2016. p. 281–302.

[64] Snape J. Marine and Offshore Cyber Briefing: Threat Case Studies. Nettitude; 2019. Available from: https://cdn2.hubspot.net/hubfs/3021880/Ebook%20PDFs/NETT_2019_MO_TCS%20EC.pdf.

[65] Hacking attack in Port of Barcelona;. Accessed: 2020-03-20. Available from: https://www.securitynewspaper.com/2018/09/26/hacking-attack-in-port-of-barcelona/.

[66] BBC. San Diego port hit by ransomware attack. BBC; 2018.

[67] Coolfire. Iranian Hackers Indicted for Port of San Diego Cyberattack. The Maritime Executive; 2018.

[68] Greenberg A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired; 2018. Available from: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[69] Juliano M. Maritime braces for the next cyber breach. TradeWinds; 2018. Available from: https://www.tradewindsnews.com/safety/maritime-braces-for-the-next-cyber-breach/2-1-437319.

[70] State-sponsored hackers spied on Denmark;. Accessed: 2019-11-25. Available from: https://www.thelocal.dk/20140922/denmark-was-hacked-by-state-sponsored-spies.

[71] Miller R. Telematics Solutions in Maritime and Inland Waterway Transport. Cambridge University Scholar; 2019.

[72] Maritime Cyber-risks. Copenhagen, Denmark: CyberKeel; 2014.

[73] Nguyen L. Collaboration in the Shipping Industry: Innovation and Technology. KNect365; 2018. Available from: https:

//knect365.com/article/pdfs/91705d00-6d9d-4ba3-98a4-9b10c92ad520_Shipping2030_report_Feb16-2018_.pdf.

[74] Police warning after drug traffickers' cyber-attack;. Accessed: 2019-11-25. Available from: https://www.bbc.co.uk/news/world-europe-24539417.

[75] Global Maritime Issues Monitor 2018; 2018. Available from: https://www.globalmaritimeforum.org/global-maritime-issues-monitor-2018.

[76] Refsdal A, Solhaug B, Stølen K. Cyber-risk management. In: Cyber-Risk Management. Springer; 2015. p. 33–47.

[77] ISO/IEC 27001:2013 — Information security management systems. International Organization for Standardization; 2013.

[78] Papastergiou PN S, Karantjias A. CYSM: An innovative physical/cyber security management system for ports. In: International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer; 2015. p. 219–230.

[79] Rocchetto M, Ferrari A, Senni V. Challenges and Opportunities for Model-Based Security Risk Assessment of Cyber-Physical Systems. In: Resilience of Cyber-Physical Systems. Springer; 2019. p. 25–47.

[80] Chertoff M. The cybersecurity challenge. Regulation & Governance. 2008;2(4):480–484.

[81] Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology; 2018. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[82] Polatidis N, Pavlidis M, Mouratidis H. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. Computer Standards & Interfaces. 2018;56:74–82.

[83] Tonn KJZL G, Czajkowski J. Cyber risk and insurance for transportation infrastructure. Transport Policy. 2019;79:103–114.

[84] Toregas C, Zahn N. Insurance for cyber attacks: The issue of setting premiums in context. George Washington University. 2014;.

[85] Meyer-Larsen N, Müller R. Enhancing the Cybersecurity of Port Community Systems. In: International Conference on Dynamics in Logistics. Springer; 2018. p. 318–323.

[86] Guide to the General Data Protection Regulation. United Kingdom; 2018. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

[87] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union. 2016;L 194:1–30.

[88] ICC Cyber Security Guide for Business. International Chamber of Commerce; 2015.

[89] MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management. International Maritime Organization (IMO); 2017.

[90] Identity Management and Cyber Security. IALA; 2020. Available from: https://maritimeconnectivity.net/docs/Identity%20Management%20and%20Cyber%20Security.pdf.

[91] Resolution MSC.428(98) Maritime Cyber Risk Management In Safety Management Systems. International Maritime Organization (IMO); 2017.

[92] Karlsson J. The Future of Maritime Cybersecurity. Secure State Cyber; 2019. Available from: https://securestatecyber.com/cyberbloggen-en/the-future-of-maritime-cybersecurity/.

[93] The EU cybersecurity certification framework; 2019. Available from: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework.

[94] Regulation (EU) 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment. Official Journal of the European Union. 2019;L 198.

[95] International Ship and Port Facility Security Code. International Maritime Organization; 2003. Available from: http://www.imo.org/en/about/conventions/listofconventions/pages/default.aspx.

[96] Common Criteria; 2017. Available from: https://www.commoncriteriaportal.org.

[97] UNCTAD: 7 Key Trends Impacting the Shipping Industry's Future. World Maritime News; 2018.