Cyberwatch Finland

WHITE PAPER 2026

MARITIME CYBERSECURITY

Cybersecurity is Built by Small Actions and Management of Large Concepts

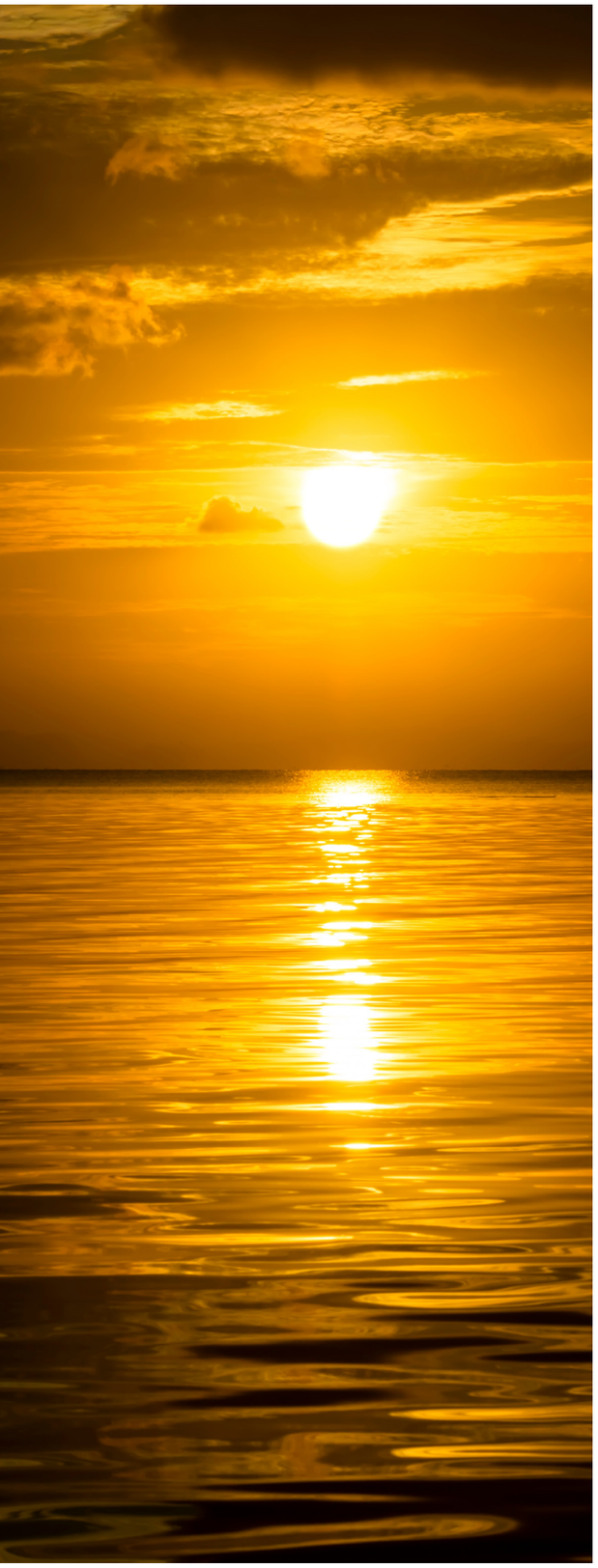


TABLE OF CONTENTS

1 Summary 4

2 Introduction 5

3 Cyber Threat Management Process 6

3.1 Maritime Transportation System (MTS) 7

4 Ship Systems 9

4.1 Ship Computer Based System 10

4.2 Ship Propulsion and Machinery Systems 11

4.3 Ship Bridge Systems 12

4.4 Vessel Operational Technology Systems 14

4.5 Ship to Shore Interface 15

5 Port System 16

5.1 Port Services and Operations 17

5.2 Port Stakeholders 18

6 Cyber Vulnerabilities in Maritime Systems 19

6.1 Vulnerability Definition 20

6.2 Ship System Vulnerabilities 20

7 Cyber Threats Against Maritime Systems 22

7.1 Threat Model-Based Motivation 23

7.2 Cyberattack Vectors 24

7.3 Cyberattack Operations and Impacts 26

8 Assessments of Maritime Cybersecurity 30

8.1 Maritime Security Management System 30

8.2 Risk Assessment Principles 31

8.3 Multi-Layer Maritime Cybersecurity Framework 33

8.3.1 The Guidelines on Maritime Cyber Risk Management 33

8.3.2 The Guidelines on Cybersecurity Onboard Ships 34

8.3.3 Maritime Cybersecurity Defence in Depth 35

8.4 Cyber Resilience Management Process 38

8.4.1 Situational awareness 39

8.4.2 Asset and Resource Management 40

8.4.3 Incident Management 40

8.4.4 Preparedness and Continuity Management 40

8.4.5 Training and Competence Management 40

8.4.6 Continuous Improvement 40

9 Future Developing Maritime Cybersecurity 41

9.1 Threat Environment is Changing 41

9.2 Artificial Intelligence and Autonomy 42

9.3 Digital Convergence 42

9.4 Harbour Digitalization 42

9.5 Autonomous Ships 43

9.6 Satellite Positioning and Maritime Cybersecurity 43

9.7 Maritime Cybersecurity Strategy Management 44

10 Conclusion 45

ANNEX 1 – Cybersecurity regulations, standards and instructions 46

REFERENCES 48

Cyberwatch Finland
WHITE PAPER 2026

Cyberwatch WHITE PAPER

Cyberwatch Finland
Part of Netum Group Plc

PUBLISHER Cyberwatch Oy
Kansakoulukatu 1b
00100 Helsinki, Finland

CONTENT Director
Aapo Cederberg
aapo@cyberwatchfinland.fi

LAYOUT PuulaMedia / Mari Riepponen

ILLUSTRATIONS AdobeStock, AI GENERATED

ISSN 2490-0761 (web)

1 Summary

In the cyber world, the most important threat focuses on critical infrastructure (CI). CI encompasses the structures and functions that are vital to society's uninterrupted functioning. It comprises physical facilities and structures as well as electronic functions and services. Critical infrastructure systems comprise a heterogeneous mixture of dynamic, interactive, and non-linear elements. In recent years, attacks against critical infrastructures, critical information infrastructures and the Internet have become ever more frequent, complex, and targeted because perpetrators have become more professional. Attackers can inflict damage on, or disrupt, physical infrastructure by infiltrating the digital systems that control physical processes, damaging specialized equipment and disrupting vital services without a physical attack. Those threats continue to evolve in complexity and sophistication.

The maritime technical environment consists of the interconnected system of systems of vessels, fairway, and ports. In this environment the cybersecurity of the connections will need to be ensured. Securing the cyber aspects of interconnected system hosted by multiple stakeholders requires a system-of-systems view in cybersecurity. The maritime and port operating environments involve cyber-physical systems equipped with intelligent machines, robots, and other corresponding products. They can independently exchange information, perform different functions, and control each other.

The maritime system is a markedly complex "system of systems." This white paper segments the maritime system into three discrete systems— ships, ports, and logistics. In addition to this, stakeholders form a very important group of decision makers and actors in the maritime environment.

Cybersecurity is an increasingly important topic for maritime operations due to rapid digital transformation and with that comes new threats and regulatory requirements. Maritime cybersecurity is the selection of policies, guidelines, procedures, security controls and measures, risk management actions, best practices, training, tools, and technologies used to protect maritime organizations, their environments, and their vessels.

> In recent years, attacks against critical infrastructures, critical information infrastructures and the Internet have become ever more frequent, complex, and targeted because perpetrators have become more professional.

2 Introduction

The maritime sector is a vital part of the global economy, whether it is carrying cargo, passengers, or vehicles. Ships are becoming increasingly complex and dependent on the extensive use of digital and communications technologies throughout their operational life cycle. The maritime transportation system is a geographically and physically complex and diverse system consisting of waterways, ports, and intermodal landside connections (DHS, 2014; Lehto, 2020).

The maritime transport sector is highly exposed to cyberattacks. Poor cybersecurity could lead to significant loss of customer and/or industry confidence, reputational damage, potentially severe financial losses or penalties, and litigation affecting the companies involved. Vessels do not need to be attacked directly. An attack can arrive via a company's shore-based information technology systems and very easily penetrate a ship's critical onboard operational technology systems. These systems are used for a variety of purposes, including access control, navigation, traffic monitoring, and information transmission. Although the interconnectivity and utilization of the cyber systems facilitate transport, they can also present opportunities for exploitation, contributing to risk for the maritime systems (DHS, 2014; Lehto, 2020).

Maritime cyber risk refers to a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures because of information or systems being corrupted, lost or compromised. Cyber risk management means the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders (IMO, 2017a).

There are currently several cybersecurity solutions and technical tools available to meet the needs of organizations. They also present challenges such as the fragmentation of technology, problems at the practical level of implementation and maintenance of new security elements, and measures may lead to an increase in the complexity of the entire functional system and the difficulty of managing the whole. (Pöyhönen, 2020).

The increasing complexity of technology and systems therefore requires the development of integrated security procedures that identify both external and internal threats. Therefore, appropriate security solutions and security breach detection procedures and a comprehensive cybersecurity system is needed to ensure the continuity of the organization's operations. (Kovanen et.al, 2018)

System thinking enables a holistic view of the organization's cybersecurity. A comprehensive view of cybersecurity is available through cybersecurity systems thinking.

This white paper applies to the Cybersecurity and Resilience Architecture Framework. It consists of three processes: Cyber Threat Management, Cyber Risk Management and Cyber Resilience Management. (Lehto and Pöyhönen, 2026)

The following figure 1 illustrates the holistic cybersecurity process.

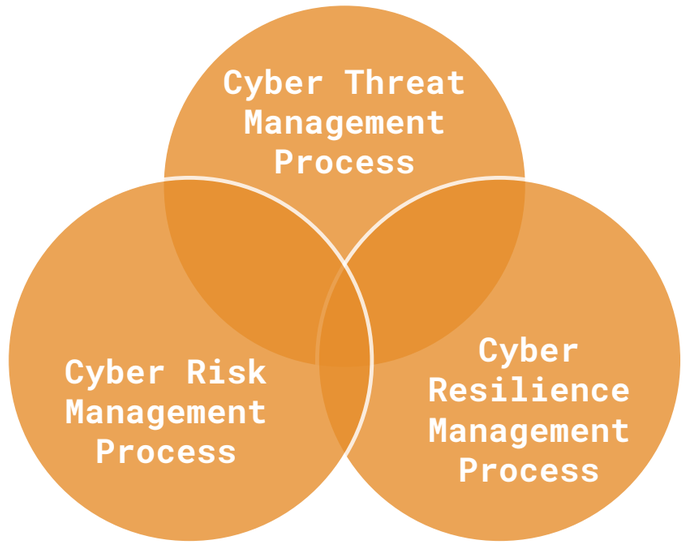


Figure 1. Cybersecurity and Resilience Processes.

3 Cyber Threat Management Process

A system of systems (SoS) methodology is particularly relevant for protecting critical infrastructure (CI) from malicious attacks and unpredictable incidents. This approach fosters a comprehensive perspective on the organization's cybersecurity. Integrating SoS into cybersecurity initiatives can strengthen overall security by considering people, processes, and technology as interconnected components. It necessitates an in-depth understanding of both the organization's operations and business workflows, treating them as holistic elements and inseparable constituents of CI entities in the digital environment. CI organizations are responsible for monitoring a broad spectrum of cyber threats and defense scenarios, regardless of their direct identification within risk management frameworks. (Lehto and Pöyhönen, 2026)

There are now numerous cybersecurity solutions and technical tools designed to address organizational needs. However, these options can also present challenges, including fragmented technology and practical difficulties in implementing and maintaining new security measures. As a result, the overall operating system may become more complex, making it harder to manage effectively. (Pöyhönen, 2020)

As technology and systems become more complex, it is essential to establish integrated security protocols capable of recognizing both external and internal threats. Implementing robust cybersecurity measures, breach detection procedures, and a comprehensive cybersecurity framework is necessary to safeguard the continuity of organizational operations. (Kovanen et.al, 2018)

The cyber threat management process (see Figure 2) generates varying levels of information tailored to the organizational hierarchy. At the strategic level, senior leadership receives relevant insights; operational-level information is provided to those responsible for daily decisions; technical or tactical-level information targets personnel who require immediate, practical data. The process encompasses system description, cyber threat analysis, vulnerability assessment, cyberattack modelling, and impact evaluation. Its outputs are subsequently utilized as inputs for the cyber risk management process. (Lehto and Pöyhönen, 2026)

Figure 2. Cyber threat management process.

3.1 Maritime Transportation System (MTS)

Maritime System of systems (SoS) is the viewing of multiple, dispersed, independent systems in context as part of a larger, more complex system. A system is a group of interacting, interrelated and interdependent components that form a complex and unified whole. The goal of a SoS view is to get maximum value out of a large system by understanding how each of the smaller systems work, interface and are used. Such designs require systems thinking -- a holistic approach to the cybersecurity analysis that focuses on the comprehensive cybersecurity in the maritime environment.

Maritime environments and vessels are more often targeted for cyberattacks. Due to the increasing digitalization of the maritime environment and the increased use of network-connected information technology (IT), operational technology (OT) systems, industrial control systems (ICS) and satellite-based services, maritime environments are susceptible to attacks by cyberattackers with different motivations. (HVK, 2021)

Maritime digital transformation is accelerating, widely embracing automation including in the traffic systems. With approximately 50,000 – 60,000 vessels at sea or in port at any one time, the deeply digitized maritime sector is highly vulnerable to cyberattacks by nation-state and criminal attackers. Vessels do not need to be attacked directly. The International Maritime Organization (IMO) reacted quickly in introducing guidelines in response to terrorist attacks on shipping but has arguably been slower in formulating appropriate cybersecurity regulations. The maritime sector appears still to be ill-equipped to deal with such future challenges as the cybersecurity of fully autonomous vessels. (Forbes, 2018)

The Maritime Transportation System, a geographically and physically complex and diverse system, consists of:

- Ship manufacturing,
- Shipping companies,
- Maritime operators,
- Ports and harbours,
- Logistics operators,
- Customers and other stakeholders.

(DHS, 2014; Bronk and DeWitte, 2022)

With approximately
50,000 – 60,000
vessels at sea or in port at any one time, the deeply digitized maritime sector is highly vulnerable to cyberattacks by nation-state and criminal attackers.

The MTS and maritime sector comprise the following components:

- Seaport operations, including vessel control and traffic management, personnel management and screening, passenger management and passport control, Wi-Fi and physically wired networks.
- Cargo and shipping, including logistics, supply chain, routing, scheduling, tracking loading/ offloading, and loss management.
- Manufacturing, supply chain, payment systems, software, and hardware.
- Vessel traffic management, including ship management, routing, communication, location management and communication.
- Shipping line operations, including passenger information, reservation systems, communication, baggage and cargo handling, maintenance, catering, and payment systems.
- Vessel operations, including the ship's onboard network architecture providing interconnection between bridge navigation, communication, mechanical, ship monitoring and security, cargo handling and other specialized systems, and communication with external networks with regards to vessel traffic management, ports, and shipping lines.
- Unmanned/autonomous vehicles, including remote control and monitoring systems.

(IMO, 2017b; Kessler, 2019)

So, the MTS technical environment constitutes a complex global network integrating a range of vessels, fairways, and ports. Ensuring cybersecurity across these interconnected systems, which are hosted, owned, and operated by various stakeholders, necessitates adopting a comprehensive system-of-systems perspective. Maritime and port operations incorporate cyber-physical systems equipped with advanced machinery, robotics, and related technologies. These systems have the capacity to generate and share information autonomously, execute multiple tasks, and exert mutual control.

These functions make the maritime sector an attractive target for hackers. According to a 2022 USCG Cyber Command report, the importance of cyber hygiene, detection, and response is rising rapidly. That year, maritime cyber incidents increased by 68%, prompting the USCG to intensify its enforcement of cyber regulations at maritime facilities. (Johnson, 2022)

MTS should be seen as a system of systems, where independent IT and OT components interact to form a unified, complex whole. This approach aims to maximize value by understanding how each component functions and connects. Systems thinking is essential for comprehensive maritime cybersecurity analysis. (Kessler and Shepard, 2022)

The maritime sector's digital transformation has led to widespread cloud adoption to manage personnel information, enterprise resource planning (ERP), customer relationship management (CRM), and other corporate functions. IT refers to the technical assets that are used in managing information processing, including software, hardware, and communication technologies (Loomis et.al, 2021).

The following chapters 4–7 present the port and ship environments and their associated vulnerabilities, cyber threats and the impact of cyberattacks.

4 Ship Systems

Ships are increasingly using systems based on digitalization, integration and automation, which require cyber risk management on board. Ships are also increasingly using systems that rely on an Internet connection to operate. Thus, extending the attack surface of vessels and exposing new vulnerabilities in these cloud-based connections. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet. (BIMCO et.al., 2017; Pijpker and McCombie, 2026)

Vessels are becoming more reliant on digitized and interconnected systems to support the different onboard systems. Vessels are also increasingly using systems that rely on an Internet connection to operate. Thus, extending the attack surface of vessels and exposing new vulnerabilities in these cloud-based connections.

Ship systems are used to manage or control the cyber-physical systems on a ship which may include access control systems; management systems; goods handling systems; energy management systems; propulsion and navigation systems; fire, communications, safety, and security systems; and those used to manage the ship's business.

A ship is a complex cyber-physical engineered system that encompasses both waterborne activities and systems, and remote elements such as navigation signals. A ship comprises five main asset types (i.e. plant and machinery, operational technology, information technology, radio frequency (RF) communications, and navigation systems) that are used to provide a range of operational services and where technology plays an increasingly important role. (Lehto, 2020)

4.1 Ship Computer Based System

A Computer Based System (CBS) refers to a programmable electronic device, or a set of interoperable programmable electronic devices, structured to accomplish one or more designated objectives, such as the collection, processing, maintenance, utilization, sharing, dissemination, or disposal of information. CBSs on board encompass both IT and OT systems. A CBS may comprise multiple subsystems interconnected through a network. Onboard CBSs can be linked directly or via public communication channels (e.g., the Internet) to CBSs located ashore, on other vessels, or at other facilities. (IMO, 2025)

Digital technologies, including CBS, have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. In some cases, these systems are to comply with international standards and the Administration's requirements.

Relevant systems could include, but are not limited to:

1. **Bridge systems:**
   - bridge systems are not always connected to other networks.
   - including navigation systems, ship safety systems, communications systems, ship-port interfaces ECDIS, GNSS, AIS, VDR and Radar/ARPA etc.
2. **Cargo and loading management systems:**
   - digital systems used for the loading, management and control of cargo, including hazardous cargo, may interface with a variety of systems ashore, including those of ports, marine terminals and stevedores.
   - bunkering, lubrication, ballast and other pumping handling and management systems.
3. **Propulsion and machinery management and power control systems:**
   - digital systems to monitor and control onboard fuel, machinery, propulsion, power control and steering.
   - vulnerability of these systems can increase when used in conjunction with remote condition-based monitoring and/or are integrated with navigation and communications equipment on ships using integrated bridge systems.
4. **Safety and security systems:**
   - systems used to maintain and to support access control to ensure the integrity, safety and security of the ship and its cargo.
   - access control and surveillance systems, load monitoring systems, safe load indicators and limiters, anti-collision systems, and shipboard security alarm and electronic "personnel-on-board" systems.
5. **Passenger service and management systems:**
   - digital systems for property management, boarding and access control.
   - provide services/facilities to passengers and to maintain the health and wellbeing of both passengers and crew.
6. **Passenger/crew public networks:**
   - fixed or wireless networks connected to the internet, installed on board for the benefit of passengers, for example guest entertainment systems.
   - systems are not related to ship operations or passenger/crew management.
7. **Administrative and crew welfare systems:**
   - computer networks managing administrative tasks, such as payroll, logistics, documentation and providing internet/email access for crew.

(BIMCO et.al., 2024; MITAGS, 2024; IMO, 2025; KRUGER, 2025)

4.2 Ship Propulsion and Machinery Systems

Ship machinery systems form the backbone of marine operations, enabling vessels to perform essential functions such as propulsion, power generation, navigation, and cargo handling. Understanding these systems is crucial for cadets, engineers, and maritime professionals, as well as enthusiasts seeking insight into the heart of marine engineering. Ships comprise various interconnected systems that support operations and safety.

Key systems include:

1. **Propulsion System:**
   - comprise diesel engines, gas turbines, or electric drives, this system propels the ship.
2. **Power Generation and Distribution System:**
   - generates and distributes electrical energy throughout the vessel.
3. **Steering System:**
   - includes rudders, hydraulic pumps, and steering gears.
4. **Bilge and Ballast Systems:**
   - handle water ingress and manage vessel stability.
5. **Fresh Water and Sewage Systems:**
   - provide potable water and waste treatment.
6. **Firefighting and Safety Systems:**
   - ensure onboard safety through detection and suppression tools.
7. **Navigation and Communication Systems:**
   - Include radar, GPS, AIS, ECDIS, GMDSS, SATCOM, VSAT, radios etc.

(Oceum, 2026)

Ships are increasingly using systems that rely on digitization, integration, and automation, which call for cyber risk management on board. As technology continues to develop, information technology and operational technology onboard ships are being networked together – and more frequently connected to the internet. (BIMCO et.al, 2018)

Figure 3 illustrates ship machinery and bridge systems.

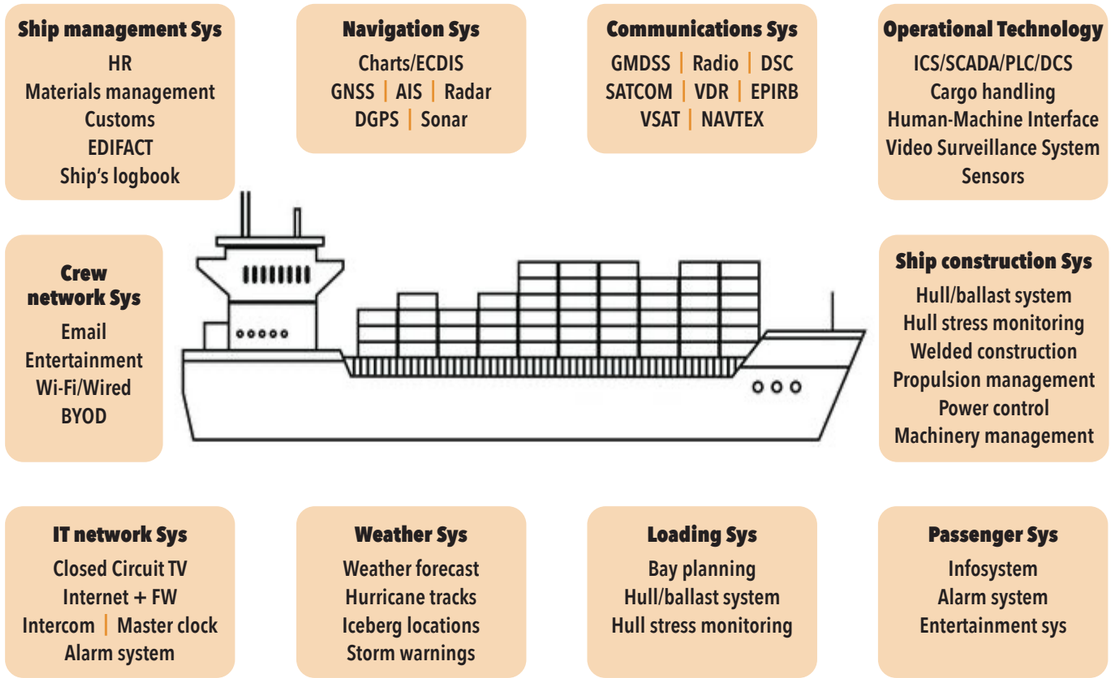


Figure 3. Ship machinery and bridge systems.

4.3 Ship Bridge Systems

Ship bridge systems are centralized, interconnected devices, workstations and their producing services that manage navigation, command, and control and safety and security on a vessel. They form Integrated Bridge Systems (IBSs). The following presents the key ship bridge systems.

GLOBAL MARITIME DISTRESS SYSTEM (GMDSS)

Global Maritime Distress System (GMDSS) is a mandatory international safety system using satellite and terrestrial technology for automated, ship-to-shore distress alerting.

INTEGRATED NAVIGATION SYSTEMS (INS)

Integrated Navigation Systems (INS) comprise the hardware and software technology in the bridge of the vessel where all functions related to navigation and communication. INS includes among others Electronic Chart Display and Information System (ECDIS), radar, Automatic Identification Systems (AIS), sonar, NAVTEX. Global Navigation Satellite Systems (GNSS) deliver precise timing and positioning. (Akpan et.al., 2022)

AUTOMATIC IDENTIFICATION SYSTEM (AIS)

Automatic Identification System (AIS) is an automated tracking system to monitor vessel location, speed, and identity in real-time. Operating on VHF bands, it broadcasts data to nearby ships and, via satellite, to shore stations, enhancing situational awareness and preventing collisions. It is mandatory for most commercial vessels, providing crucial information like vessel name, Course Over Ground (COG), Speed Over Ground (SOG), and navigation status.

MARITIME VERY SMALL APERTURE TERMINAL (VSAT)

Maritime Very Small Aperture Terminal (VSAT) is for high-speed data transmission rates throughout maritime operations. VSAT acts as two-way satellite ground station for satellite data transmission and offers a variety of communication and security services, like voice, and video connectivity.

ELECTRONIC CHART DISPLAY AND INFORMATION SYSTEM (ECDIS)

Electronic Chart Display and Information System (ECDIS) is a mandatory, computer-based, navigation system that uses Electronic Navigational Charts (ENCs) and real-time sensor data (GPS, gyro, radar, AIS) to assist mariners with route planning and monitoring. It enhances safety by providing continuous, automated positioning, anti-grounding alarms, and, when used properly, acts as a primary navigation tool. (Akpan et.al., 2022)

DIFFERENTIAL GPS (DGPS)

Differential GPS (DGPS) is an enhancement to standard GPS that improves positional accuracy from 15 meters to 1–3 meters (or centimeters with specialized systems).

SHIP RADIO SYSTEMS

Ship radio systems are critical communication tools for maritime safety and operation, primarily comprising VHF (Very High Frequency), MF/HF (Medium/High Frequency), and satellite systems. Modern vessels use these for Distress calling, ship-to-shore, and ship-to-ship communication, with many complying with the Global Maritime Distress and Safety System (GMDSS) for automated emergency alerting via DSC (Digital Selective Calling).

SATELLITE COMMUNICATION (SATCOM)

Satellite communication (SATCOM) uses orbital satellites as relays to receive, amplify, and transmit radio signals for voice, data, and video, providing global connectivity, particularly in remote areas.

NAVTEX (NAVIGATIONAL TELEX)

NAVTEX (NAVigational TEleX), sometimes styled Navtex or NavTex, is an international automated medium frequency direct-printing service for delivery of navigational and meteorological warnings and forecasts, as well as urgent Maritime Safety Information (MSI) to ships.

LIGHT DETECTION AND RANGING (LIDAR)

Light Detection and Ranging (LiDAR) in ships enhances maritime situational awareness by using laser pulses to create, in real-time, high-resolution 3D, 360-degree, or 180-degree maps of the surrounding environment.

Table 1. A summary of the main ship systems. (Akpan et.al., 2022)

	SYSTEMS	USE
NAVIGATION	Automatic Identification System (AIS)	- Vessel traffic monitoring and assistance. - Avoid a collision. - Notify ports and maritime authorities of the ship's location. - Calculate the distance between the ship and the other ships. - Ensure sea safety by monitoring traffic. - Accident investigation and search and rescue operations.
	Electronic Chart Display Information System (ECDIS)	- Collect and combine data from electronic navigation sensors. - Shows the position of the ship in real time.
	DGPS and GNSS	- Displays the position of the ship. - Differential GPS improves positional accuracy from 15 meters to 1–3 meters. - Displays the speed, the route and time. - Provides a timestamp.
	Radar	- Provides information about the ship's surroundings. - Detection of the position and speed of objects.
	Sonar	- Uses sound propagation to navigate, communicate, or detect objects.
	Light Detection and Ranging (LiDAR)	- Enhances maritime situational awareness by using laser pulses to create, in real-time, high-resolution maps of the surrounding environment.
	Laser Detection and Ranging (LADAR)	- It is a combination of laser and radar produces an image by scanning a very high repetition rate laser rangefinder over a scene to produce a three-dimensional map.
	Speed log sensors	- Measures speed relative to water (Speed Through Water - STW) or the seabed (Speed Over Ground, SOG). - Includes Electromagnetic (EM) logs, and Doppler logs.
	Gyroscopic stabilizer	- Reduces a vessel's roll by using a rapidly spinning, heavy flywheel to produce counteracting angular momentum.
COMMUNICATION	Radio systems	- Consists of VHF (Very High Frequency), HF (High Frequency) and MF (Medium frequency), and satellite systems.
	Digital Selective Calling (DSC)	- is a VHF/HF/MF radio standard that allows mariners to send automated, location-tagged distress alerts to the Coast Guard and other vessels.
	Global Maritime Distress System (GMDSS)	- Broadcast the distress messages related to safety issues - Sending and receiving critical safety alerts.
	Very Small Aperture Terminal (VSAT)	- Uses a satellite network to send and receive data. - Offer a variety of communication and security services.
	Satellite communication (SATCOM)	- Uses orbital satellites as relays to receive, amplify, and transmit radio signals for voice, data, and video. - Provides global connectivity, particularly in remote areas or during emergencies.
	Emergency Position Indicating Radio Beacon (EPIRB)	- Maritime safety device which operates worldwide. - Provides GPS-accurate location data to authorities and often includes a homing signal.
	A Voyage Data Recorder (VDR)	- Is mandatory, "black box" system. - Fitted on ships to record, secure, and store data on the vessel's position, movement, and bridge audio.
	NAVTEX	- Is automated medium frequency direct-printing service for delivery of navigational and meteorological warnings and forecasts, as well as urgent Maritime Safety Information (MSI).

	SYSTEMS	USE
OTHER SYSTEMS	Global Industrial Control Systems (ICSs)	- Assist in reducing human errors. - Increase resource productivity. - Extend the life of the equipment. - Control and monitor parameters on board a ship.
	Propulsion and machinery management and power control systems	- Monitor and regulate onboard machinery. - Monitor and regulate propulsion. - Monitor and regulate steering.
	Video Surveillance System	- Monitor transport operations in large storage areas. - Monitor transport operations in large vessels.
	IT Network Systems, intercom, CCTV, master clock	- Used for internal/external processes to send, receive, and store data. - Used for crew personal devices (BYOD).
	Passenger information system	- Provides announcements and information to passengers. - Includes a warning and alarm system. - Provides entertainment and payment services.
	Loading Systems	- Includes bay planning, hull/ballast system and hull stress monitoring services.
	Weather System	- Gives weather forecast, hurricane tracks, iceberg locations storm warnings.
	Electronic Data Interchange for Administration, Commerce, and Transport (EDIFACT)	- It is an international standard for exchanging structured business documents electronically. - It acts as a universal, paperless, and automated systems.

4.4 Vessel Operational Technology Systems

Operational Technology (OT) manages industrial operations through computing systems, supporting both human and machine interfaces to enhance efficiency and automation. OT includes Industrial Control Systems (ICS) that connect equipment and software for cyber-physical tasks such as power management, engine support, data logging, cargo control, sensors, pumps, hydraulics, cranes, and on-board monitoring. (deWitte and Lehto, 2025)

In the ship environment OT systems control the physical world, and IT systems manage data. OT refers to the hardware, systems and software that operate your vessels as well as monitors/controls physical devices and processes. The use of OT—where embedded computers directly control hardware—throughout ports and ships enables smart maritime systems. OT also includes supervisory control and data acquisition (SCADA) systems, such as flow computers, transport and transfer systems, and monitoring meters, which play a crucial role in the global transportation of oil and natural gas. (Loomis et.al, 2021)

Industrial Control Systems (ICSs) serve as the critical interfaces that translate virtual commands into tangible actions within industrial settings. ICSs facilitate real-time, bidirectional data exchange among sensors, workstations, and other networked devices across a system. Through this integration, they enable ongoing, distributed monitoring and control of operational processes.

ICS consists of SCADA systems, Distributed Control Systems (DCS), and Programmable Logic Controller (PLC) software. SCADA handles software operations, while DCS connects controllers, sensors, operator terminals, and actuators to manage processes efficiently. These systems enable both human and machine interaction with industrial operations for greater automation. Even if applications or operational technology are compromised, they may continue functioning normally. (Weed, 2017; Securicon, 2019; Karamperidis et.al, 2021)

These systems enable both human and machine interaction with industrial operations for greater automation.

Figure 4 illustrates the environment of ICS, SCADA, DCS and OT.

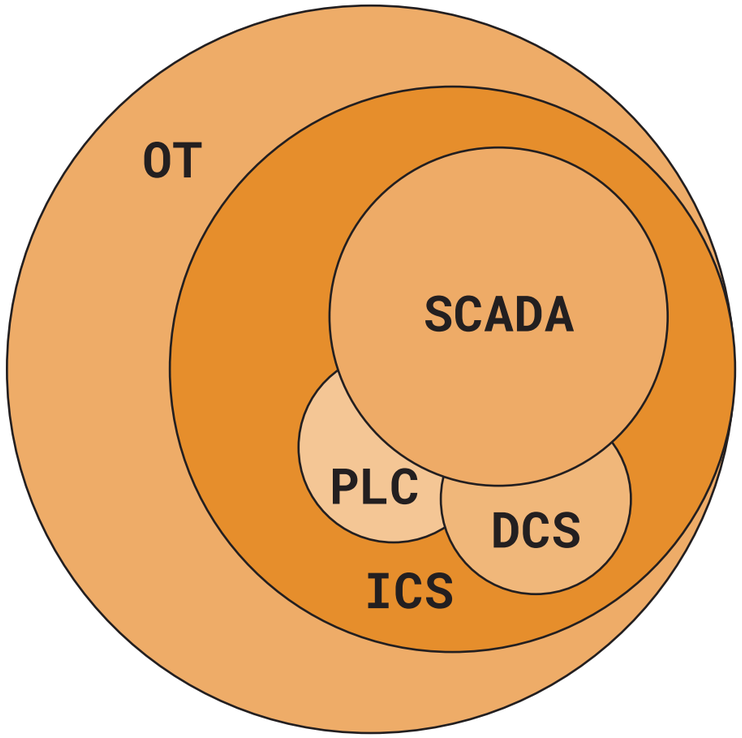


Figure 4. Environment of ICS, SCADA, DCS and OT. (formulated from Securicon, 2017)

4.5 Ship to Shore Interface

Ships are now closely linked with shoreside operations through digital communication for business, operations management, and contact with head offices.

Key systems for navigation, power, and cargo are increasingly digital and internet-connected to support various functions such as:

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

(BIMCO et.al., 2024)

The above list provides examples of this interface and is not exhaustive. The above systems contain, process and exchange data, which may be of interest to cyber criminals to exploit.

5 Port System

A port is a cyber environment with land and waterside operations. As shown in Figure 5, it consists of four main assets—buildings, linear infrastructure, plant and machinery, and information and communications systems—that support its services, with technology playing a growing role. (IET, 2020)

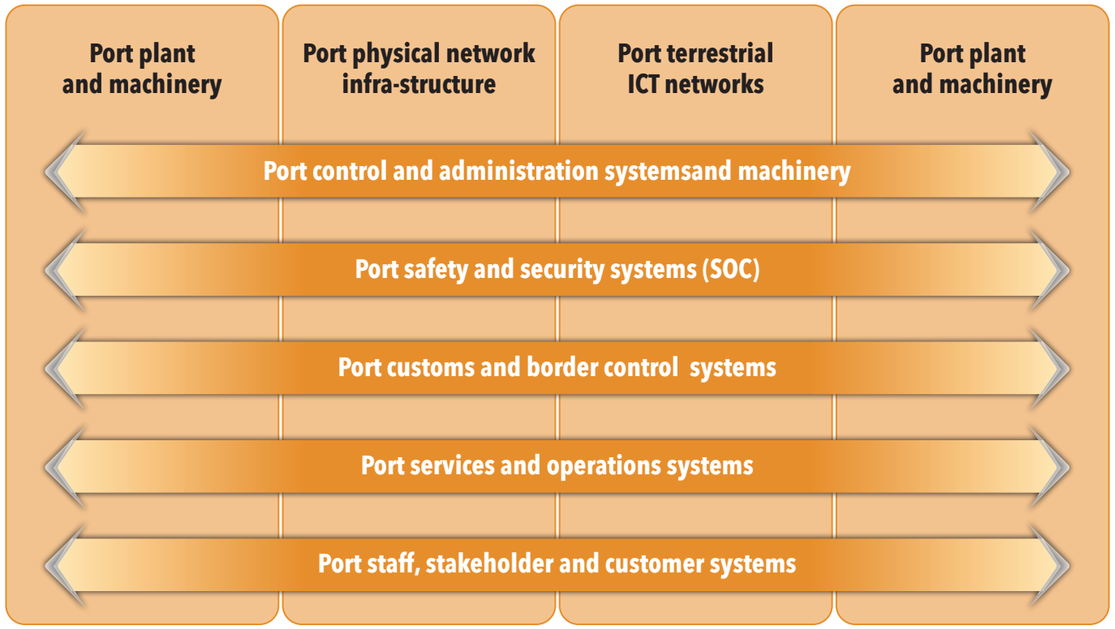


Figure 5. Main port systems.

In maritime transport, sea areas are divided into port approach zones and port areas. Ships entering a port from open sea must navigate shallow waters, narrow channels, environmental challenges, and heavy traffic. Once docked, vessels load or unload cargo, vehicles, or passengers. Effective port operations require cooperation among stakeholders and logistics systems, while land transportation is an integral part of port facilities. (Simola and Pöyhönen, 2022)

Ports link land and sea transport for passengers and freight. Port terminals are where these journeys begin, end, or transfer, serving as key points in transportation. They need specialized facilities and equipment to manage their traffic. (Rodrigue and Slack, 2020)

A port is defined as any maritime facility that is operated on a commercial basis and has at least one or more wharves for docking ships.

For a port to function, it must have these core services:

1. An administrative department that oversees everything,
2. Infrastructure and structures for landing, loading, offloading, and exiting,
3. Security installations for ensuring safety,
4. Emergency cover in case of a crisis,
5. State of the art communication systems to consult with other sites,
6. Government installations such as customs and immigration,
7. A customer service centre to deal with and process clients.

(Maure, 2018)

Port cybersecurity is essential to ensuring the safe and secure operation of ships at sea and onshore. Ports serve a critical function in facilitating domestic and international supply-chain activities by connecting sea and inland transport services. Ports represent complex ecosystems where assets and systems are increasingly integrated and interconnected, resulting in service-based interdependencies and voluminous data exchanges that occur every day. (ENISA, 2020)

5.1 Port Services and Operations

Port services include a wide variety of maritime and logistical support activities that are vital for moving ships and cargo safely and efficiently. These essential services cover cargo handling (such as loading and unloading), drayage, storage or warehousing, pilotage, towing, and sometimes refuelling and technical maintenance. By providing these functions, ports effectively link ocean carriers with inland transportation systems and play a key role in supporting international trade.

Core port services and operations are:

- CARGO HANDLING — Loading, unloading, and transferring cargo between vessels and land transport.
- PORT LOGISTICS & STORAGE — Providing open and covered terminal areas for cargo.
- VESSEL SERVICES — Including fairway pilotage, towing, mooring.
- SAFETY AND SECURITY — Maintaining port traffic safety.
- TRANSPORTATION & TRANSLOADING — Moving cargo between different transportation modes and trucking services that transport containers from the port.
- MAINTENANCE & SUPPORT — Providing spare parts, technical training, and equipment repairs for port machinery.

The Shore Control Center manages ship operations and security from land. It features Human Machine Interfaces for ship control, as well as a Remote Maneuvering Support System that provides information on autonomous procedures. In Finland, Vessel Traffic Services (VTS) include systems like GOFREP, a mandatory ship reporting tool, and monitor traffic through radar and AIS technology. Both traffic data and VHF communications are recorded. Weather operators collect sensor data, process it in a forecasting environment, and share it with other relevant systems. (Kovanen T., Pöyhönen J., Lehto M. 2021b)

Terminals maintain the flow of goods and people in port operations and serve as essential transfer points between transport modes. Buses, cars, trucks, and rail all deliver passengers and freight to ports for ship loading, making terminals necessary passage points. (Rodrigue and Notteboom, 2020)

Infrastructure and services are for passengers and vehicles on ships and other operations (e.g. passenger gangways, parking, restaurants and bars, border control, etc.). In a similar way, staying services are provided for vehicles and passengers: parking, passenger lounges, luggage handling facilities, restaurants and bars, shopping malls, etc. The passengers pass through the port areas to go up in the cruise ships and ferries (ENISA, 2019).

Activities related to vehicles transport with dedicated infrastructure and services to welcome vehicles on ships and manager related operations. This includes RoRo (Roll-on/roll-off ships) activity as cargo is on trucks. The cargo is shipped in containers, trucks, trailers, and other similar large units.

5.2 Port Stakeholders

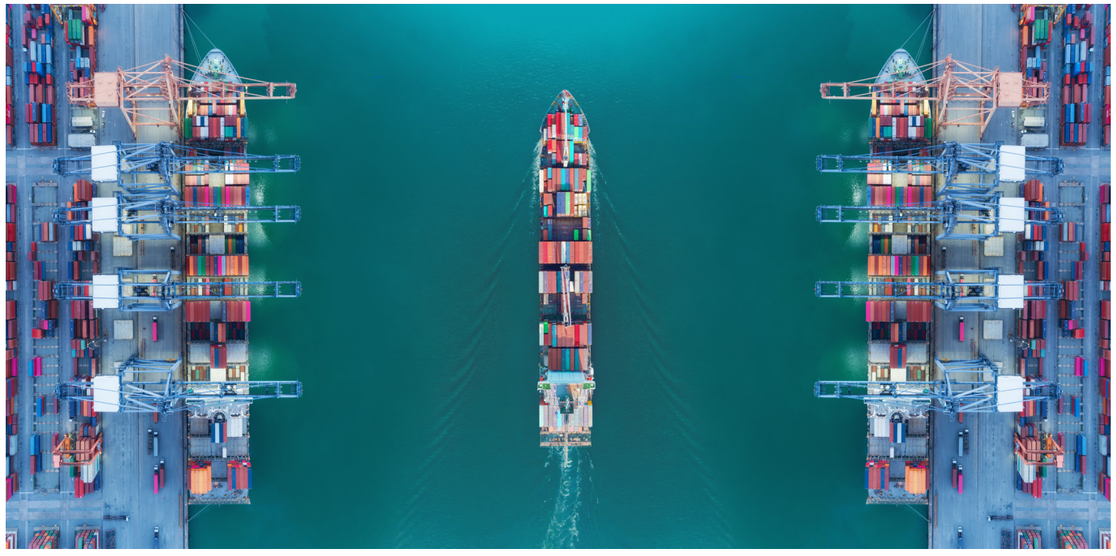
Port stakeholders are a diverse group of actors—including port authorities, terminal operators, shipping lines, labour unions, government agencies, and surrounding communities. ENISA has made a high-level overview based on the stakeholder's main roles. They are two main categories: Port authorities and terminal operators. (ENISA, 2019)

Port authorities:

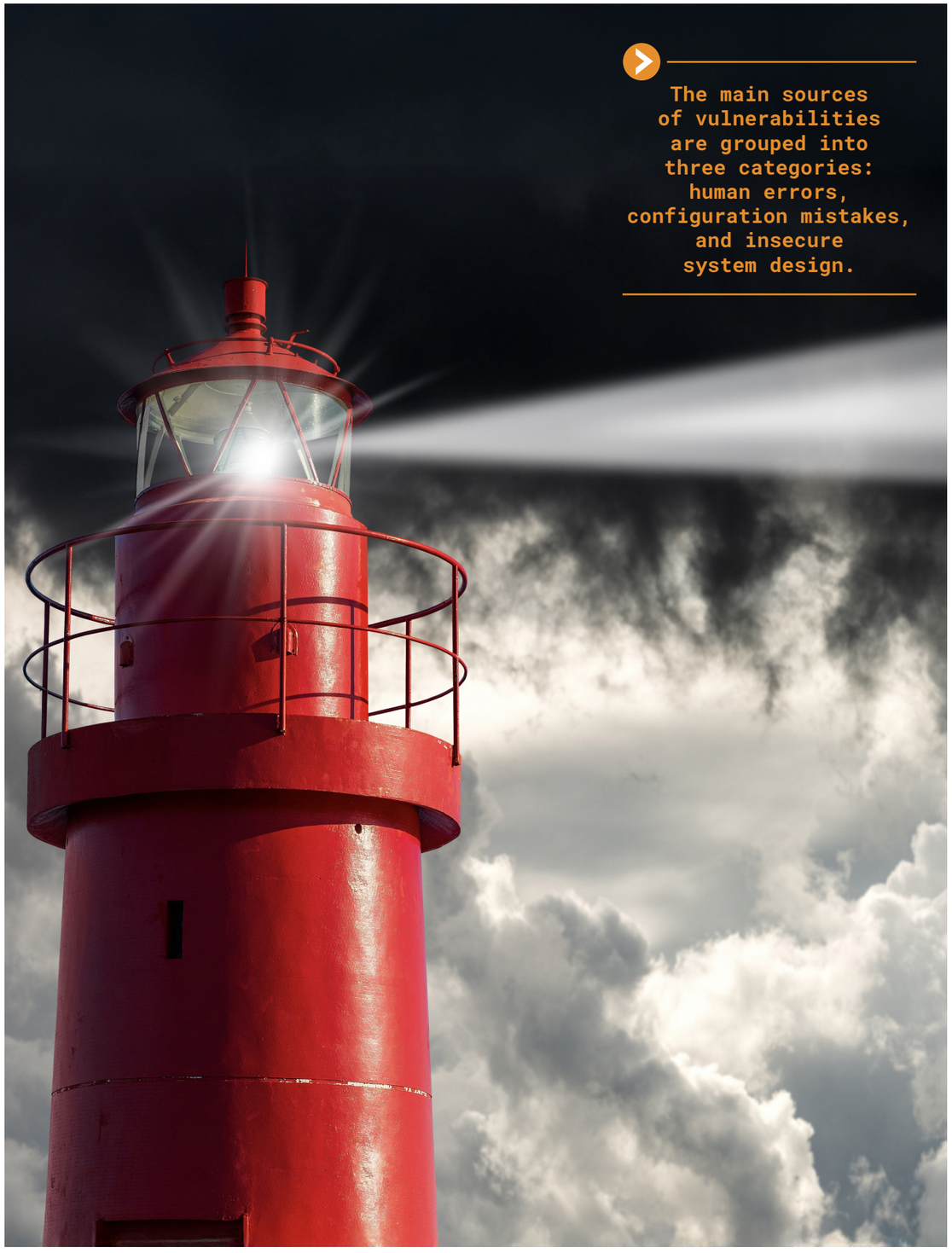
- Harbor master,
- Safety and security,
- Administration and finance,
- Marketing and communications,
- Infrastructure and OT management,
- Environmental and territorial management,
- IT and cybersecurity,
- Logistics.

Port terminal operators:

- Administration and finance,
- Marketing and communications,
- Infrastructure and OT management,
- IT and cybersecurity.



6 Cyber Vulnerabilities in Maritime Systems



The main sources of vulnerabilities are grouped into three categories: human errors, configuration mistakes, and insecure system design.

6.1 Vulnerability Definition

Vulnerabilities can result from weaknesses in security procedures, software applications, policies, or regulatory compliance. A vulnerability is an intrinsic flaw that raises the likelihood of an incident or worsens its effects. These weaknesses threaten maritime systems as much as land-based ones. Every critical infrastructure has unique vulnerabilities in its IT and OT systems. The main sources of vulnerabilities are grouped into three categories: human errors, configuration mistakes, and insecure system design. (Weed, 2017)

Vulnerability can be defined as an exploitable weakness or deficiencies in a system, device or its design that allow cyberattackers to execute cyberattacks (Bertino et al., 2010). Vulnerabilities may be the outcome of a weakness in system security procedures, software applications, policies and procedures and regulatory compliance. Vulnerability is the inherent weakness in the system which increases the probability of an occurrence or exacerbates its consequences.

Vulnerabilities can be divided into those that exist in:

1. **People's actions,**
2. **Processes in the organizations,**
3. **Technologies.**

1. PEOPLE refer to the human resources available at the firm's disposal. The people are the ones who do the tasks described in the process. Most cybersecurity threats are due to employee errors. For example, a report by Kaspersky Lab indicated that employee errors accounted for 90% of the data breaches that occurred in the cloud. Employees are often victims of social engineering tactics and may end up unknowingly providing attackers with login credentials or classified organization data. (Hess, 2019) So, quite often human actors are the weakest link in cybersecurity.

2. PROCESSES are crucial in defining how the organization's activities, roles and documentation are used to mitigate the risks to the organization's information. Process vulnerabilities among others are lack of written security policy, poor regulation policy, lack of security awareness and training, and poor adherence to security, lack of access control and non-existence of disaster/contingency plan. But processes are nothing if people do not follow them correctly. (FCC, 2014) Once the people and processes are in place, organizations should define the cybersecurity technology to support them.

3. TECHNOLOGY solutions protect against cyber risks that may arise from network vulnerabilities, but technology itself contains vulnerabilities (hardware, HW and software, SW). So, technological vulnerabilities are security holes in a system.

Software vulnerability is a bug in program coding, configuration, or management. A program can be an algorithm, application, operating system, or browser and control software like communication protocols and devices drives. Hackers use vulnerabilities in software attacks to force systems to give them access to unauthorized data, execute malicious code, obtain remote control, or cause the system to spread infections (Chong, 2013).

Hardware is the bottom level component of systems that are critical to critical infrastructure. Hardware vulnerability is an exploitable weakness in a computer system that enables attack through remote or physical access to system hardware. Hardware vulnerabilities are exceedingly difficult to identify. In January 2018, the entire computer industry was put on alert by two new processor vulnerabilities, dubbed Meltdown and Spectre, which defeated the fundamental OS security boundaries separating kernel and user space memory. The MTS would not have been immune and might have been affected, but shipping firms are notoriously secretive about such attacks, making the overall system hard to defend. (Constantin, 2021).

6.2 Ship System Vulnerabilities

Cyber vulnerabilities in ship systems often stem from older, interconnected technologies—for example, outdated operating systems that haven't been patched, poor password practices, and insufficient separation of networks. Critical vulnerabilities are often located in operational technology (OT), such as navigation systems (GPS/AIS), propulsion systems, and cargo control systems. These vulnerabilities enable and target ransomware, state-sponsored attacks, and data theft. (Securewest, 2026)

Table 2 Main vulnerabilities in ship bridge systems. (Akpan et.al., 2022)

Table 2. Main vulnerabilities in ship bridge systems. (Akpan et.al., 2022

SYSTEM	WEAKNESS	ATTACK VECTOR	CONSEQUENCES
AIS	- Signal interference - No or weak encryption	- Jamming or spoofing - False information sharing - Malware attack	- Ship hijacking - Destruction or theft of data
ECDIS	- Outdated operating system (OS) - Insecure update medium	- Hacking - Data manipulation - Ransomware	- Loss of communication - Ship hijacking - Data theft - Compromising computers
GNSS and GPS	- Weak signal strength - Signal interference	- Jamming or spoofing	- Ship hijacking - Navigation problems - Disrupt vessel operation
Radar	- Weak interference tolerance and evasion ability	- Jamming or spoofing	- Navigation problems - Maritime accident, grounding
GMDDS		- Jamming or spoofing	- Wrong position of the ship - Further attacks on ECDIS
ICS	- Inadequate Access Control Management - Information exposure - Poor patch management - Hardware failures - Improper security configuration - Lack of network segmentation - Weak password policies - Lack of firewalls - Lack of encryption - Weak remote access policies - Weak USB policy - Lack of training for SOS	- Malware attack - Phishing - Exploiting legacy systems - Software manipulation	- Ship hijacking - Unavailability of the ICS - Data leakage - Physical damage to facilities - Interference with safety systems - Unplanned shutdowns - Damage to equipment
Propulsion and machinery management and power control systems	- SW vulnerabilities - HW vulnerabilities	- Malware attack - DoS/DDoS attacks - Smuggling - Stealing - Manipulation attacks	- Ship hijacking - Diversion of the ship - Propulsion system could be interrupted - Ship damage - Financial damage - Disclosure of sensitive data
Very Small Aperture Terminal (VSAT)		- Fake signals - Malware attack - Stealing	- Theft of sensitive data - Upload of malware - Change of GPS coordinates
IT network systems	- Poor access control - Weak password policies - Poor patch management - Improper security configuration - Poor security documentation - Lack of network segmentation - Lack of firewalls - Lack of encryption - Weak remote access policies - Weak USB policy - Lack of training for Secure Operations of the Systems	- DoS/DDoS attacks - Malware attacks	- Upload malware - Unauthorized physical access - Unauthorized logical access - Loss of confidential documents - Financial damage - Theft of sensitive data - Reputation damage

The onboard systems consist of potentially vulnerable equipment, which should be reviewed during the assessment.

The vulnerability assessment can be assisted by answering the below questions for each system:

- Is the system stand-alone or is it connected to other systems?
- Is the system connected externally, either directly or via other systems?
- Does the system have effective, built-in risk mitigation measures such as e.g. encryption?
- Does the system require regular software updates?
- Does operating the system allow connecting removable devices, for example to obtain diagnostic information?
- Is the system easy to access physically?

(BIMCO et.al., 2024)

7 Cyber Threats Against Maritime Systems

The motives can be reduced to their very essence: egoism, anarchy, money, destruction, paralysis, and power.

7.1 Threat Model-Based Motivation

A classification model for six threats based on motivational factors: cyber vandalism, cybercrime, cyber espionage, cyber terrorism, cyber sabotage, and cyber warfare. The motives can be reduced to their very essence: egoism, anarchy, money, destruction, paralysis, and power. The model was modified from Myriam Dunn Cavelty's structural model (Dunn Cavelty, 2010; Ashenden, 2011; Lehto, 2013).

The motivation affects the attacker's targeting and methods. While a vandal seeks visibility by defacing a website, a spy wishes to stay unnoticed to gain information. Therefore, being motivated does not mean that an attack is possible for the attacker. Understanding the motivations and capabilities of different archetypes limits the number of scenarios and thus makes evaluation feasible for the defender.

The parameters of the attacker archetypes in maritime environment are presented in Table 3 Attributes of the attacker archetypes. Capability is derived from Bodeau, McCollum and Fox (2018), and impacts are derived from Mitre (2020, 2022a), and Kovanen, Pöyhönen, Lehto, (2021a) and Simola, Pöyhönen, Lehto (2023).

Table 3. Attributes of the attacker archetypes.

	VANDALISM	CRIME	ESPIONAGE	TERRORISM	SABOTAGE	WARFARE OPERATIONS
Motivation and goal	Trying to make political change based on personal political or ideological motives. Egoism gain	Making money through fraud or from the sale of valuable information. Financial gain	Gaining an economic, political, or military advantage. Information gain	Gaining social instability and influencing political decision-making. Anarchy gain	Causing instability, chaos, political change, and infrastructure paralysis. Paralysis gain	Performing a destructive attack on a nation's critical infrastructure. Political or military dominance
Target	Digital services of governments and companies, individuals' information systems	Digital services of governments and companies, individuals' information systems	Data and information about governments and companies	Data and information about governments and companies. Critical infrastructure	Nation's critical infrastructure	Nation's critical infrastructure (civilian or military).
Capability	Acquired Attackers with moderate or limited expertise	Augmented Attackers with moderate or limited expertise	Advanced Attackers with very sophisticated or moderate expertise	Advanced Sophisticated attackers, capable of multiple, coordinated attacks	Integrated Very sophisticated attackers, capable of multiple, coordinated, continuous attacks	Integrated Very sophisticated attackers, capable of multiple, coordinated, continuous attacks
Trigger	A social event, an action of a company or an individual	The opportunity for economic gain	The need for political, economic, and military information	Cultural, nation's political or military actions	Testing own offensive cyber-attack capabilities, preparing hybrid or military operations	Achieving political or military objectives through military cyber operations
Impacts	ICT: Defacement ICT: Network Denial of Service ICS: Loss of Productivity and Revenue	ICT: Data Encrypted for Impact (ransom) ICT: Resource Hijacking (mining cryptocurrencies) ICS: Manipulation of Control (cargo capture at port)	ICS: Theft of operational information	ICS: Loss of Safety	ICS: Damage to Property (shipwreck)	ICS: Denial/ Manipulation of View (GNSS attacks) ICS: Denial/Loss/ Manipulation of Control (controlling ship) ICS: Damage to Property (shipwreck)

7.2 Cyberattack Vectors

An attack vector is the specific pathway, method, or technique—such as phishing emails, malware, or software vulnerabilities—that threat actors use to gain unauthorized access to a computer, network, or system. These vectors exploit weaknesses in an organization's attack surface to deliver a payload, steal data, or cause disruption.

Potential cyberattacks towards the OT- and IT-systems can be divided into two main groups: un-targeted cyberattacks when the attacker uses tools and techniques available on the internet to locate and exploit widespread vulnerabilities and targeted cyberattacks when the attacker uses sophisticated tools and techniques specifically created for targeting a shipping company or a vessel. (Larsen and Lund, 2021)

Spoofing is the manipulation of a vessel's AIS device to hide or alter the vessel's location or identity. For example, a vessel operator may enter a false Maritime Mobile Service Identity (MMSI) number to appear to be a different vessel (identity spoofing) or change its coordinates (location spoofing). Deliberate falsification typically occurs when a vessel engages in illegal, unreported and unregulated (IUU) fishing activities, as the vessel operators attempt to conceal their true activities. (Cutlip, 2016)

Here are some of the most prevalent cyber threats facing maritime security:

PHISHING AND SPEAR-PHISHING ATTACKS — These involve deceptive emails and messages designed to trick maritime staff into revealing sensitive information or downloading malware. Phishing attacks can lead to unauthorized access to the ship's systems and sensitive data.

MALWARE AND RANSOMWARE — Malicious software can be used to disrupt the operations of onboard systems, steal sensitive data, or lock out legitimate users, often demanding a ransom to restore access. Ships are particularly vulnerable when they integrate their systems with port and logistics services that may not have robust cybersecurity measures.

GPS SPOOFING — Attackers may manipulate GPS signals to mislead maritime navigation systems about the vessel's location or route. This could potentially lead to accidents or unauthorized detours.

GPS JAMMING — Attacker can overwhelm global navigation satellite systems (GNSS) receivers with powerful radio signals that drown out the signals from navigation satellites. This could potentially lead to accidents or unauthorized detours.

DENIAL OF SERVICE (DOS) AND DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS — These attacks overload a ship's networks with traffic, making them unable to process legitimate requests and potentially leading to operational failures.

UNAUTHORIZED ACCESS AND INSIDER THREATS — Unauthorized access can occur through inadequate security measures, allowing hackers or even insiders to manipulate or steal data. Insider threats also include sabotage by disgruntled employees who have access to the systems.

RANSOMWARE ATTACKS — These occur when malware encrypts a victim's files, making them inaccessible unless a ransom is paid. In the maritime sector, ransomware can lock down navigation systems, access digital logs, or other critical data, severely disrupting maritime operations.

SUPPLY CHAIN COMPROMISES — This threat involves a malicious actor infiltrating the maritime sector through less secure elements in the supply chain. For example, a compromised software update or hardware component can be used to gain access to wider network systems used in maritime operations.

DATA BREACHES — Unauthorized access to confidential data can be devastating. For maritime operations, this could involve access to cargo details, ship schedules, or personal information of crew members, potentially leading to operational manipulations or piracy.

IMPERSONATION — Attackers may pose as legitimate users or officials to gain access to secure systems. In maritime settings, impersonation could involve posing as port officials, ship inspectors, or other entities that have authorized access to sensitive operational data.

SOCIAL ENGINEERING — Social engineering is a technique used by cyber-criminals to manipulate the humans behind machines rather than exploiting code-based vulnerabilities. This can be done by impersonating legitimate parties, targeting vulnerable individuals, building trust with a victim, creating a sense of urgency in a message, and more.

(Darktrace, n.d.)

GNSS spoofing has become a powerful electronic warfare tool capable of manipulating positioning, navigation, and timing (PNT) data across civilian and military systems, maritime navigation is highly dependent on the GNSS system. According to C4ADS report "Above Us Only Stars – Exposing GPS Spoofing in Russia and Syria" large-scale activity has already been observed. Investigations identified 9,883 suspected spoofing incidents affecting 1,311 vessels across Russia, Crimea, and Syria between 2016 and 2018. It was also observed that civilian systems are highly vulnerable because commercial GNSS receivers lack the protection mechanisms found in encrypted military navigation systems. (C4ADS, 2019)

Figure 6 shows the top 10 threats. The three largest slices are all related to exposed land-based IT-infrastructures that the maritime sector depends on. (Meland et.al., 2021)

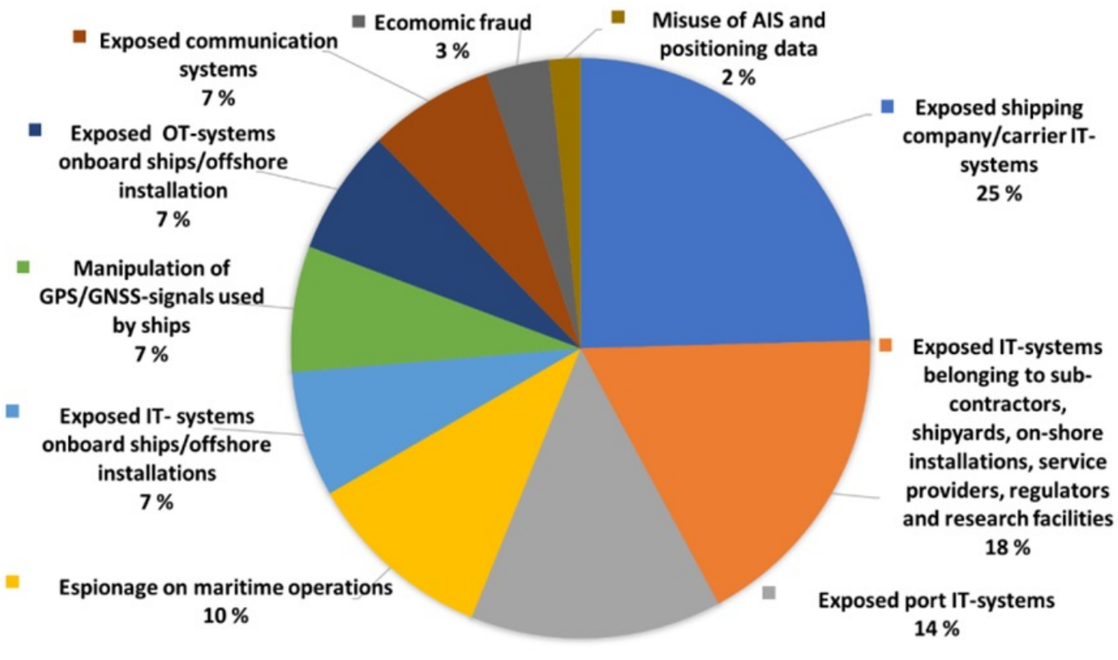


Figure 6. Top 10 maritime sector cyber threats. (Meland et.al., 2021)

7.3 Cyberattack Operations and Impacts

Cyberattack operations constitute coordinated, typically multi-phase campaigns that target digital systems, networks, or infrastructure for purposes such as espionage, financial gain, or disruption. These activities are predominantly carried out by state-sponsored entities or cybercriminals who leverage vulnerabilities through methods including phishing, malware, and ransomware, resulting in substantial harm or intelligence theft. (Kovanen, Pöyhönen and Lehto, 2021b)

In an ICS environment, the MITRE framework uses the terms denial, loss, and manipulation. Denial is a condition which occurs only while the attack is active. Loss refers to sustained loss of an asset that continues after the active malicious interaction has ceased. Manipulation alters the asset and can be either loud and easy to detect or subtle and longer sustained. Table 4 illustrates different cyberattacks and their impacts. (Kovanen, Pöyhönen, Lehto and 2021b)

Table 4. Types of attacks and their impacts.

Account access removal	Removing account access prevents operators from using locked systems or accessing their information, for example VTS.
Data destruction	Data destruction, encryption, disk wiping, and service stoppage all render data and services unusable. Targeting system structures, such as disks, can disable entire systems rather than just data. In maritime contexts, destroying chart information is one example.
Data manipulation	Data manipulation renders original information inaccessible and is harder to detect if subtle. Operators may continue working but make decisions based on false data; for example, manipulated location details can cause a ship to go off course.
Defacement	Defacement usually affects websites but the impacts on an organization are wider. These include damage to reputation, disruption to normal routines, potential data breach, potential diversion for other attacks and increased downtime. As defacement can make the official information unavailable or manipulate it, there can be delays in finding the relevant information in time critical situation. For example, if a website is the only location for VTS contact information, a defacement will hinder the incoming vessel's operations.
Denial of Service	Denial of Service attacks disrupt either the endpoint or its network, rendering the service unusable. Dependent systems also face issues, though deploying alternatives can lessen the impact. The urgency depends on the system's role.
Firmware corruption	Firmware corruption refers to an attack designed to make systems unusable or unable to start by tampering with BIOS or other device firmware. These attacks may provide lasting access for further actions or be timed to disrupt operations. Information and communication technology systems on ships and in ports are potential targets for such threats.
Inhibit system recovery	Inhibiting system recovery constrains the restoration of systems impacted by various factors. The level of threat posed by this supporting impact increases in proportion to the time sensitivity of the affected system. Consequently, it is essential to assess not only the security of primary systems but also the robustness of their recovery strategies.
Manipulation of Control	Manipulation of Control describes a situation in which an adversary can issue unauthorized commands or alter system settings to cause further harm, such as property damage. For example, the Industroyer malware can directly operate switches and circuit breakers at power grid substations. This impact is particularly hazardous in cyber-physical system (CPS) environments, including those found in ships and ports.
Manipulation of view	Manipulating data is a subtler attack than simply denying or losing access to information, as slight falsifications are harder to spot than missing data. Operators may act on false information, losing situational awareness. For example, if a water depth sensor gives inaccurate readings with no backup or other sensors for verification, ships might be directed into shallow areas, risking shipwreck.
Data breach	The theft of operational information impacts systems containing stored data or participating in data flows. While the objective is not to modify data within these systems, successful breaches of security controls during such theft may expose them to additional forms of attack.

The following Table 5 shows the attack type and effect against ports.

Table 5. Cyberattack vectors and impacts against ports.

TARGET	TIME	ATTACKER	ATTACK VECTOR	IMPACT
Port of Antwerp, Netherlands	June 2013	Criminal group	Intrusion by sending emails with attachments containing Trojans and then installing key logger to capture passwords.	Attackers took control of the computers of two container terminals and of a harbour company with the aim smuggling drugs unnoticed from the port.
Port of Barcelona, Spain	Sep 2018	Unknown	Ransomware, Ryuk	Targeted internal servers. Affected internal land operations and its systems, disrupted e.g., loading and unloading of boats. Transport operations stopped.
Port San Diego, USA	Sep 2018	Iranian Cybergang	Ransomware, Sansam	Malware infiltrated ports computer network and was disrupting administration systems. The main impact was on the issuing of park permits, public records requests and general business services.
Port Vancouver, Canada	Oct 2018	Unknown	DDos + Brute force attack	Affected sending many work requests in the systems. 225 000 user accounts were propped. Wi-Fi-connected computers caused the spread of the virus. Networked and connected computers were affected.
Port of Marseilles, France	Mar 2020	Hacker group Mespinoza	Ransomware, Mespinoza/Pysa	Maritime infrastructures were not directly targeted but were incidentally affected due to their interconnection with information systems in Aix-Marseille-Provence, which was the main target of the attack.
Port of Kennewick, USA	Nov 2020	Unknown	Sophisticated ransomware attack, using military-grade encryption	Attack paralyzed computer servers and email systems. Attackers demanded a $200,000 ransom, which the port refused to pay.
Transnet, South-Africa	July 2021	Russia?	Ransomware, Death Kitty	Attack disrupted TransNet's container and trucking operations at several key container terminals, including Port of Durban, Ngqura, Port Elizabeth and Cape Town.
Port of Houston. USA	Aug 2021	Nation-state actor	Data breach	Attackers broke into one of the port's web servers, then attackers exploited a vulnerability in ManageEngine ADSelfService Plus, a password management tool and installed malicious code to expand their access to the system. No operational data or systems were impacted.
Port of Nagoya, Japan	2023	Pro-Russian hackers	Ransomware	Attack shutting the port for two plus days and causing major manufacturers like Toyota to suspend operations temporarily.

The following Table 6 shows the attack type and effect against maritime operators.

Table 6. Cyberattack vectors and impacts against maritime operators.

TARGET	TIME	ATTACKER	ATTACK VECTOR	IMPACT
Several maritime companies and ports.	June 2017	Russia, Sandworm	Ransomware-attack. NotPetya encrypts files with extensions from a hard-coded list.	The variant infected the IT-systems of the world's largest shipping company Moller-Maersk with 600 container vessels handling 15% of the world's seaborne trade in Port of Los Angeles, Port of Rotterdam, Port of Long Beach. Also, Chinese shipping company COFCO Group. Maersk reporting up to $300 million in losses
Australian shipbuilder and defence contractor Austal	2018	Unknown	Cybersecurity breach and extortion attempt	The Austal data management system had been targeted by an offender. Some staff email addresses and mobile phone numbers were accessed. The attacker tried to sell some of the stolen material online and engaged in extortion.
Shipping company CMA CGM, French	Sep 2020	Ragnar Locker Gang	Ransomware	Cybercriminals stole personal data from clients using the Ragnar Locker ransomware and demanded a ransom before giving the data back to the company.
Hyundai Merchant Marine, South Korea	June 2021	Unknown	Phishing	Due to a phishing attack, a virus was able to infiltrate the email systems. Email servers in all areas except for America and Europe impacted by the unauthorized security breach, so that the email system could not be used.
K-line, Japan	March and July 2021	Unknown	Hacking. Unauthorized access to the overseas subsidiary systems.	The first stemmed from malware that infiltrated the company's IT network. The second attack was unauthorized access to overseas subsidiary systems.
Shipping company CMA CGM, French	Sep 2021	Unknown	Data breach	Data breach following a cyberattack that compromised limited customer information. The leaked data included customer names, employers, job titles, email addresses, and phone numbers.
Swire Pacific Offshore, Singapore	Nov 2021	Unknown	Combined ransomware and data breach	The incident involved a ransomware attack that allowed unauthorized actors to access and steal data from company IT systems, resulting in the theft of confidential commercial information and personal data.
Hellmann Worldwide Logistics	Dec 2021	Unknown	Ransomware,	Attack compromised servers and triggered a shutdown of central data centre to prevent further spread. The attack significantly disrupted operations for weeks, leading to a stolen data leak of roughly 70 GB and subsequent phishing risks.
Several cargo shipping companies in Europe	2024	Mustang Panda, China	RansomExx	The attacker deployed Korplug loaders via USB drives containing suspiciously named files, resulting in compromised systems across Norway, Greece, and the Netherlands. While several malware samples were successfully blocked, others employed modified signatures and exploited DLL hijacking techniques.

The following Table 7 shows the attack type and effect against ships.

Table 7. Cyberattack vectors and impacts against ships.

TARGET	TIME	ATTACKER	ATTACK VECTOR	IMPACT
German-owned container ship	Feb 2017		The attack targeted the navigational system, likely through vulnerabilities in the ship's IT or satellite communications	Hackers gained full control of a German-owned container ship's navigation system for 10 hours. The pirates aimed to force the vessel into a specific zone to hijack it. The crew could not steer the ship.
Several ships	2018	Unknown	Several incidents were reported where Electronic Chart Display and Information System (ECDIS) units on ships were infected by viruses and malware.	Attack caused significant navigational risks and operational delays. Infections often occurred via infected USB sticks used for chart updates or through connections with compromised onboard networks, resulting in the failure of navigation systems at sea.
Bulk ship	2018	Unknown	Malicious code	Following the bunkering operation, a bunker surveyor came aboard the vessel and asked to use a computer in the engine control room so they could print paperwork for signing. When the surveyor plugged in a USB drive, malware was accidentally introduced into the ship's administrative network.
Hurtigruten cruise line	Dec 2020	Unknown	Ransomware	The attack forced the company to shut down most of its systems. An unauthorized actor compromised the computer systems associated with two of their ships, the MS Fram and the MS Midnatsol. The attacker got customers' personal information - names, dates of birth, passport numbers and passport expiration dates.
Two ships	2019/ 2020	Lazarus' hacker group	Ransomware, Hermes 2.1	Attack infected both ships' network, including multiple workstations on the administrative network getting. The infection came as a macro-enabled Word document attached to an email.
Several ships	Mar 2025	Anti-Iranian government hacktivist group Lab Dookhtegan	Communication disruption	Hacktivist group disrupted communications on over 100 oil tankers associated with Iranian government-linked company. They exploited vulnerabilities in the ships' satellite communication systems, such as VSAT terminals.

The information in Tables 5-7 has been gathered from the following sources: Safety4Sea, 2018; Meland et al., 2021; BIMCO et.al. 2021; Akpan et.al, 2022; Pijpker and McCombie, 2026.

The most extensive in terms of economic impact was the NotPetya attack in 2017. On Tuesday, June 27, 2017, the NotPetya malware emerged as a highly destructive and significant threat to the global shipping industry. NotPetya caused approximately $10 billion in damage and significant loss of goods, services and business opportunities. The Petya variant specifically infiltrated the IT systems of Maersk, the world's largest shipping company. Maersk operates 600 container vessels and manages 15% of global shipping. This disruption affected all of Maersk's business units, including container shipping, port and tug operations, oil and gas production, drilling services and oil tanker management, with reported losses reaching up to $300 million. (Gronholt-Pedersen, 2017)

Maersk operates 600 container vessels and manages 15% of global shipping.

8 Assessments of Maritime Cybersecurity

8.1 Maritime Security Management System

There are several key issues that make cybersecurity for the maritime sector particularly complex and challenging. There are many different classes of ships, tugs, and boats, all of which operate in very different environments. These vessels tend to have different computer systems built into them. Many of those systems are designed to last no more than three decades. Placed in another context, many ships operate outdated and unsupported operating systems, which are the ones most prone to cyberattacks (Forbes, 2018).

Researcher from Australian Maritime College presents the model of the Maritime Security Management System (MSMS). It is a framework designed to strengthen security in maritime logistics beyond the International Ship and Port Facility Security (ISPS) Code, focusing on shore-based activities, personnel, and risk mitigation. It often emphasizes education, training, and the human factor as crucial elements for success, aiming to enhance organizational performance and resilience. By the researchers, the MSMS framework elements are activities, stakeholders, organizational relationships, security dimensions, security elements, and criteria. The attributes of the elements are in Table 8. The attributes in the table have been applied using the definitions of Vinh Thai and Devinder Grewal. (Thai and Grewal, 2007).

Table 8. Criteria of MSMS.

ELEMENT	ATTRIBUTES
Activities	• Port operation • Ship operations • Cargo and logistic operation
Stakeholders	• Port authorities • Transport and cargo operators • Government authorities • Security service providers • Shipping companies
Organizational relationships	• Between each transport operator and their security service providers • Between the government (regulator) and transport operators • Between stakeholders in the MSMS • Between port authorities within the organization regarding security accountability and responsibility • Between each transport operator and their stakeholders
Security dimensions	• Security awareness education and training • Identity and Access Management • Physical security • Process security • Human security • Cyber-Physical system security • Information security • Cybersecurity
Security elements	• People • Process • Technology
Criteria **Criterion attributes describe good/ effective MSMS**	• Effective communication between all members of the security system. • Good security situational awareness. • To be holistic in the consideration of risk assessment at appropriate intervals. • Constant reviewing of security processes, procedures and available technology. • Security should become part of the wider safety management system. • Meaningful government inputs in terms of resources support and legislative guidance. • Adequate funding for security measures. • Effective compliance with regulations and administrative guidelines. • Organizing security training and exercises regularly. • Cybersecurity information exchange within the organization and between security actors. • Consistence in application of systems, processes and protocols. • Cybersecurity management should be integrated with other organizations' risk management processes. • Auditable metrics, monitoring and reporting procedures in place. • If necessary, a cybersecurity service is purchased from SOC service provider. • Cybersecurity implementation must include strategic view, operational view, and tactical/technical view.

The main objectives of MSMS are to identify maritime cybersecurity activities associated with maritime operations in the Ship and Port.

8.2 Risk Assessment Principles

Risk management has become vital due to increased security demands from digital operations, emerging technologies, and evolving threats. Effective risk management helps organizations identify and address major risks that could impact their goals or daily activities. Risk management helps organizations enhance security by targeting cost-effective measures that reduce or mitigate recognized threats. The guideline also highlights the importance of identifying opportunities, as missing them can hinder operational improvement or goal achievement. Digitalization presents a valuable opportunity for growth but brings associated risks that must be addressed. (Pöyhönen et.al., 2023)

Information flows rely on both legacy and modern technologies, and electric supply chains play a crucial role when analysing cybersecurity risks from a maritime service perspective. By recognizing these technologies, we can pinpoint various system functions, conduct risk assessments, and accurately determine residual risks. Likewise, it is essential to examine system dependencies in order to identify related security and cybersecurity risks. (Pöyhönen et.al., 2023)

Port risk assessment processes require the adoption of a comprehensive, multi-dimensional model that encompasses every layer and cyber-physical aspect of port operations.

This structured approach to risk assessment involves the following four steps:

a. **Risk Identification:** All possible sources of cyber-attacks, vulnerabilities, their causes, and potential impact are identified at this stage of risk assessment. Possible cyber-physical attack vectors in the communication and port services layer must be identified at this phase. Moreover, existing safeguards (intrusion detection system, prevention, or cyber-defensive strategies) capable of reducing or mitigating the consequences of any hazardous event must be identified.

b. **Risk Analysis:** During this stage, both the likelihood and impact of each identified risk are assessed. A single hazardous event can lead to a range of outcomes, such as port service interruptions, power utility outages, or communication system failures. It is important to consider consequences across all systems, since issues can spread from one to another—an intrusion in communications could, for example, disrupt port operations. For this reason, risk analysis must take into account every possible consequence.

c. **Risk Evaluation.** Evaluation of identified risks and their potential consequences is performed at this phase. Depending on the severity and impact, a quantitative value is assigned to every possible risk. Every risk of all port systems will be assigned a value. This value depicts the severity of all possible risk factors.

d. **Risk Handling.** Risk handling makes use of quantitative information gathered during the risk evaluation stage. Stakeholders rely on this data to create and carry out effective mitigation plans, as well as to invest in cybersecurity measures. At this phase, a variety of strategies are available, such as upgrading physical systems, deploying automated intrusion detection systems, and incorporating AI-powered cyber defence techniques.

(Pöyhönen et.al., 2023)

The proposed risk handling plan is then evaluated against financial feasibility, and only those plans are selected by stakeholders that balance costs and efforts of implementation against obtained benefits. Figure 7 illustrates the cyber risk assessment process. (Pöyhönen et.al., 2023)

Digitalization presents a valuable opportunity for growth but brings associated risks that must be addressed.

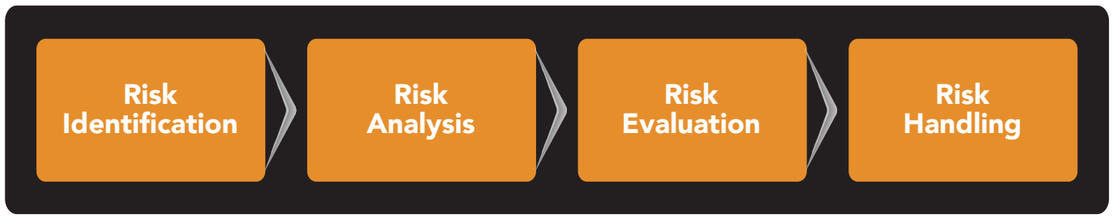


Figure 7. Cyber risk assessment process.

8.3 Multi-Layer Maritime Cybersecurity Framework

8.3.1 The Guidelines on Maritime Cyber Risk Management

The IMO Guidelines on Maritime Cyber Risk Management outline the functional elements essential for effective cyber risk management. These elements are intended to operate concurrently and continuously and should be appropriately integrated into a comprehensive risk management framework. The cybersecurity controls specified under each functional element constitute the minimum requirements that must be implemented. (IMO, 2025)

These guidelines present the functional elements that support effective cyber risk management.

The foundation of risk management is governance. According to IMO (2025):

- Establish and monitor risk management strategy, expectations and policies.
- Define personnel roles and responsibilities for cyber risk management.
- Ensure business continuity, such as backup management and disaster recovery, and crisis management.

Ports and port facility stakeholders from around the world are reporting measurable increases in cyber-threat activities. The International Association of Ports and Harbors (IAPH) alliance has produced guidelines for implementing cybersecurity in ports. The IAPH guidelines illustrate how managers should consider cyber risk in the context of their own operations. The guidelines explain how to assess the risks and vulnerabilities of port operations and how to adopt a holistic approach that allows them to organize and manage their cybersecurity program by implementing tailored cybersecurity protection, detection and mitigation measures. Creating cyber awareness among port operators and general and technical cybersecurity training for all actors is crucial. (IAPH, 2021)

Other elements of cyber risk management are:

1. **Identify:** Determine the current cyber risk to ships and ship/port interfaces.
2. **Protect:** Implement risk control processes and measures to protect CBSs, and contingency planning to protect against a cyber incident and ensure business continuity of shipping operations, human safety, safety of the vessel and/or threat to the environment.
3. **Detect:** Develop, implement and practice activities necessary to detect a cyber incident in a timely manner. Implement appropriate measures to detect unintended activity on CBS and timely identification of a cyber incident.
4. **Respond:** Develop, implement and practice activities and plans to provide resilience and to restore systems necessary for shipping and ship-port operations or services impaired due to a cyber incident. Implement appropriate measures to minimize the effect of a cyber incident detected to other parts of ship systems.
5. **Recover:** Identify and implement measures to restore onboard CBS including networks necessary for shipping operations impacted by a cyber incident.

(IMO, 2025)

In the Figure 8 illustrates Maritime Cyber Risk Management approach.

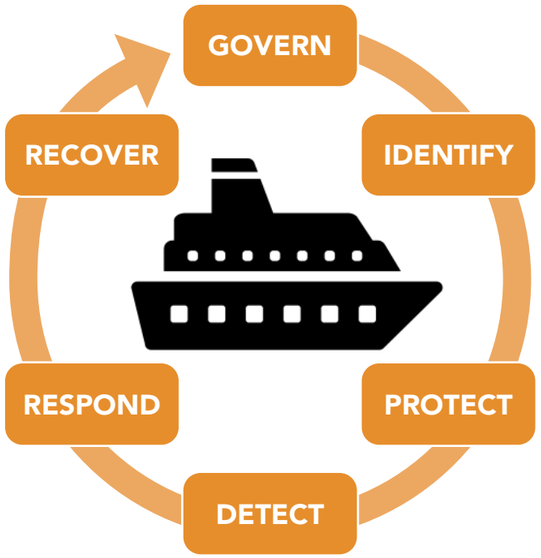


Figure 8. IMO cyber risk management approach.

8.3.2 The Guidelines on Cyber-security Onboard Ships

The Maritime industry released version 5 in 2024 The Guidelines on Cybersecurity Onboard Ships. These guidelines explain why and how cyber risks should be managed in a shipping context.

According to the guidelines, cyber risk management should be tailored to each company's risk profile, as well as meet flag-State regulatory requirements, and should furthermore:

- Identify the roles and responsibilities of users, key personnel, third parties (e.g. vendors, service providers and integrators) and management both ashore and on board.
- Identify the systems, assets, data and capabilities that, if disrupted, could pose risks to the ship's operations and safety.
- Implement technical and procedural measures to protect against a cyber incident, provide timely detection of incident, minimize the impact of incidents and ensure continuity of operations.
- Fulfil regulatory requirements.
- Ensure reporting and investigation of cybersecurity incidents according to the principles of the SMS.
- Exercise contingency and response plans regularly.

(BIMCO et.al., 2024)

In the Figure 9 illustrates the cyber risk management approach. (BIMCO et.al., 2024)

Figure 9. Cyber risk management approach. (BIMCO et.al., 2024)

8.3.3 Maritime Cybersecurity Defence in Depth

A multi-layer maritime cybersecurity ecosystem uses integrated technical, operational, and administrative controls to safeguard vessels, ports, and offshore infrastructure from digital threats. It secures IT and OT systems, data, communication, and assets, ensuring compliance with IMO and new 2025 USCG regulations. (BIMCO et.al., 2024)

Key Maritime defence-in-Depth Layers:

1. **Physical Layer:** Securing physical access to devices, servers, and networks on ships and in ports.
2. **Network Layer:** Utilizing segmentation, firewalls, and, when applicable, VLANs to isolate critical systems.
3. **Application/System Layer:** Employing anti-malware, patch management, and secure software development.
4. **Data/Information Layer:** Encrypting data at rest and in transit.
5. **Personnel/Procedural Layer:** Training crew and staff to recognize phishing, social engineering, and adhering to cyber policies.

It is important to protect critical systems and data with multiple layers of protection measures, which combine the role of personnel, procedures and technology to:

- Enhance cyber incident detection likelihood.
- Optimize resource usage to maintain data confidentiality, integrity, and availability in IT and OT systems.
- Implement system-level measures to further protect against unauthorized access.

Onboard connected OT systems should be safeguarded by multiple technical and procedural protection measures. While perimeter defences, including firewalls, play a critical role in preventing unauthorized access, these alone may not adequately address potential risks posed by insider threats.

This defence in depth approach encourages a combination of:

- Physical security of the ship in accordance with the Ship Security Plan (SSP),
- Protection of networks, including effective segmentation,
- Intrusion detection and protection,
- Use of effective firewalls,
- Periodic vulnerability scanning and testing,
- Software patching/updating and software whitelisting,
- Identity and access controls,
- Configuration and change management controls,
- Appropriate procedures regarding the use of removable media and password policies
- Personnel's cybersecurity awareness and understanding of the risk to themselves and the industry
- Understanding and familiarity with appropriate procedures, including incident response.

(BIMCO et.al., 2024)

Company policies and procedures should help ensure that cybersecurity is considered within the overall approach to safety and security risk management. The complexity and potential persistence of cyber threats means that a "defence in depth" approach should be considered. Equipment and data protected by layers of protection measures are more resilient to cyber incidents.

Core Components of a Multi-Layer Maritime Security Ecosystem are follows:

SHIP SECURITY

Implementation of IACS Unified Requirements (UR); E26 "Cyber resilience of ships" and E27 "Cyber resilience of on-board systems and equipment". These apply to nearly all ships contracted for construction on or after 1st July 2024. E26 focuses on vessel-wide, secure network integration (OT/IT) and zoning, while E27 ensures individual system components are secure. Key measures include shipboard network segmentation, robust access controls, and malware protection.

MARITIME OPERATIONAL TECHNOLOGY (OT) SECURITY

Securing critical shipboard and port systems (navigation, engine control, propulsion, cargo handling) from unauthorized access, essential for preventing disruptions to operations. Key measures include network segmentation, continuous monitoring, and access controls, and patch management.

MARITIME INFORMATION TECHNOLOGY (IT) SECURITY

Protecting vessels, ports, and cargo from cyber threats targeting information networks and systems. Key measures include network segmentation (IEC 61162-460), firewalls, encryption, IPS/IDS/SIEM, IAM-systems and multi-factor authentication (MFA).

PORT AND SHORE INFRASTRUCTURE SECURITY

Protecting maritime transportation systems (MTS), terminal operating systems, cargo and logistics, and supply-chain data from physical and cyber threats. Key measures include advanced threat detection and secure communication protocols, perimeter security, Identity and Access Management, comprehensive cyber risk management procedure.

ADMINISTRATIVE & REGULATORY COMPLIANCE

Adherence to IMO safety management systems and other national and international regulations' requirements (like IACS, EU NIS2). Key measures include designation of responsible cybersecurity personnel, cyber risk management policy, and strengthening cybersecurity expertise. Key Regulatory Drivers are IMO Resolution MSC.428(98), implemented in 2021, IACS E26/E27: Technical standards for system-level resilience (mandatory for all newbuilds with contracts signed after 1 July 2024), and EU Directive on Network and Information Systems (NIS2), implemented in October 2024

The following table 9 presents possible mitigation actions. (Akpan et.al., 2022)

Table 9. Maritime Mitigation Actions.

SYSTEMS	MITIGATION ACTIONS
Automatic Identification System (AIS)	• All AIS information should be verified. • Encryption of the VHF signals. • Integrity of broadcast information should be monitored to ensure that position and identity are correct. • Equipment that broadcasts AIS signals should be secured, and unauthorized access should not be possible. • Local navigation warnings should be considered if false AIS signals are being broadcast.
Electronic Chart Display Information System (ECDIS)	• ECDIS development should be a principle: Security by Desing and maintaining security throughout the entire life cycle. • Regular documentation, monitoring, and patching of the ECDIS framework. • ECDIS chart update should be monitored and registered, the most effective is to use physical update tools. • All upgraded files should be scanned with antivirus software before operational deployment. • ECDIs should be used on a separate network or effectively protected firewall. • Only approved staff should have physical access to ECDIS and its underlying components.
GNSS and GPS	• Device identification and authentication, using resilient, encrypted receivers. • Implementing anti-jamming antennas. • Adopting inertial backup systems. • Employing monitoring tools to detect signal anomalies.
Radars	• Device identification and authentication. • Detecting anomalies in radar data caused by cyberattacks. • Protecting against Machine-on-the-Side (MotS) attacks using radar-specific IDS approaches. • Cryptographic protection. • Information system backup.
Global Maritime Distress System (GMDSS)	• Cryptographic protection. • Device identification and authentication. • Data at rest protection secures inactive data stored on physical or cloud media. • Physical access control. • Contingency plan.
Industrial Control Systems (ICSs)	• Segmenting Industrial Control Systems (ICS) and Operational Technology (OT) from Information Technology (IT) networks (Purdue Enterprise Reference Architecture, PERA). • Cryptography or other protected methods to shield passwords. • Configuration management and patch management controls. • Protection of Internet-connected ICS devices and that passwords updating. • Password files protection against by making hashed passwords. • Strong password usage control. • Efficient remote access policy and changes management. • Blocking unnecessary USB ports. • Adequate training of system users.
Propulsion and machinery management and power control systems	• Information system backup. • Preparing to prevent denial of service attacks. • Monitoring physical access.
Very Small Aperture Terminal (VSAT)	• Encrypted communication systems. • Using managed service provider's cyber defence mechanisms. • Strict authentication and access control management. • Data at rest protection.
IT network systems	• Information system backup. • Identity, authentication and access control. • Segmentation of networks. • Ensuring threat protection mechanisms. • Promoting configuration/patch/update management system. • BYOD policy definition and control. • Cybersecurity training for all users
Human security	• Promoting cybersecurity culture within the organization. • Effective organization of cybersecurity management. • Effective Information Sharing system and collaboration organization. • Ensuring effective cybersecurity for all. • Evaluating training effectiveness with cybersecurity drills. • Promoting cyber hygiene within all stakeholders' parties.

Protective technology (Port scan, FIREWALL, IDS, IPS, SIEM) and update procedures of these solutions as well as other relevant resiliency actions, such as cybersecurity policies, are needed in daily life as well as in the use of the ICT environment. (Pöyhönen, Hummelholm and Lehto, 2022)

8.4 Cyber Resilience Management Process

The cyber environment is often unpredictable, given the complex networks of stakeholders, operational systems, and technologies involved. It is not possible to foresee every scenario during risk assessments, so it is essential to prepare and plan to manage uncertainty and strengthen cyber resilience. Cybersecurity resilience forms a core part of preparedness and business continuity management. It describes an organization's ability to defend against, detect, respond to, and recover from cyber threats. Through proactive, adaptable strategies, organizations can lessen the damage from attacks and maintain ongoing operations. Figure 10 shows elements of cyber resilience. (Lehto and Pöyhönen, 2026)

Cyber resilience encompasses not only the physical infrastructure and information present within complex networks, but also cognitive and social components. It integrates physical systems, software, and data with the conduct and activities of individuals within an organization. (Kott and Linkov, 2019)

Figure 10. Cyber Resilience Management Process.

8.4.1 Situational Awareness

Organizations require accurate information regarding their external environment and relevant events, as well as the potential effects these factors may have on their operations. Achieving a holistic perspective on cybersecurity and resilience necessitates the development of comprehensive situational awareness. Establishing effective cybersecurity situational awareness demands advanced capabilities for threat detection within cyber space. Such awareness is vital for evaluating an organization's overall cybersecurity posture and resilience, facilitating improved decision-making by incorporating observations, assessments, metrics, and analyses. This process can be approached from tactical, operational, or strategic standpoints.

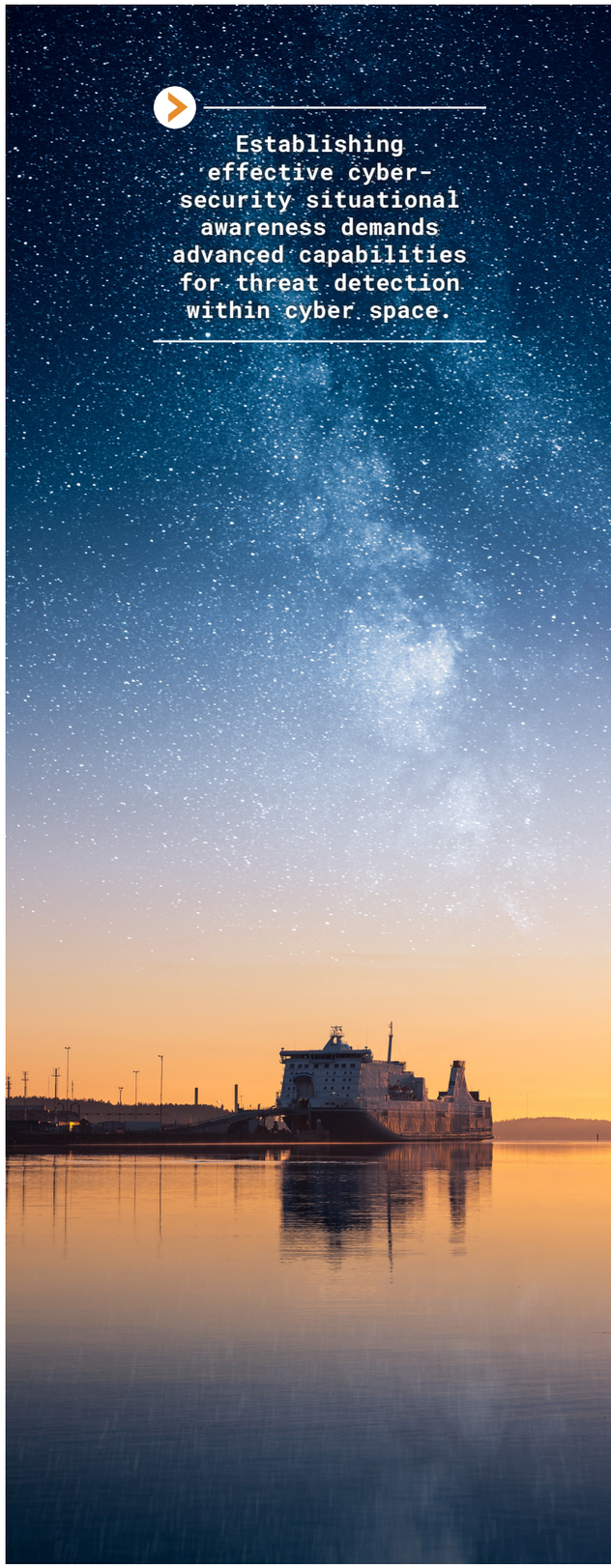
The situational picture plays two main roles. First, it gives everyone a real-time overview of the security situation and ongoing events, pulling information from observation systems, public sources, and internal channels. Second, it includes an analysis of what's happening now and predicts what might occur next. By providing details about past, current, and future events, the situational picture can be shared either as a periodic general evaluation or as an in-depth analysis of specific issues, exploring events and their consequences.

Maritime Domain Awareness (MDA) refers to a comprehensive understanding of all elements related to the maritime domain that may influence security, safety, economic interests, or the marine environment.

MDA encompasses three primary components:

- Maritime Situational Awareness
  - Based on the gathering of static and dynamic data to generate a picture of the current situation within the maritime domain.
- Maritime Threat Awareness
  - Requires the identification of the potential threat vectors that could be active within the area of interest.
- Maritime Response Awareness
  - Covers the mapping and real-time tracking of available response resources to ensure that they can rapidly be deployed to counter threats.

(IMO, n.d.a.)



8.4.2 Asset and Resource Management

Asset and Resource Management (ARM) ensure continuity and clear oversight of IT and OT resources, both in inventory and active use. It involves managing contracts, hardware, software, and configuration items by regularly assessing their value, usage, timeliness, and updates.

8.4.3 Incident Management

Incident management encompasses the processes an organization employs to analyse, identify, and resolve incidents while implementing measures to prevent future occurrences. A key aspect of incident management involves quickly determining which information and systems have been compromised by an attacker. A thorough approach to handling incidents involves spotting disruptions, assessing their impact and scope, protecting sensitive information systems, deploying backup resources, and putting isolation procedures in place to safeguard critical systems.

8.4.4 Preparedness and Continuity Management

Preparedness and continuity management ensures that organizations can withstand disruptions and maintain critical functions, security, and operations in emergency situations. Management includes a contingency plan, continuity management plan, and recovery plan.

The Preparedness Plan is an organization's tool for managing disruptions in normal and exceptional circumstances.

The Contingency Plan is a statutory requirement for public organizations. The materials from the Rescue Institute can be used in its preparation.

The Recovery Plan is a critical element of an organization's disaster management strategy. It provides a structured methodology for addressing unexpected events effectively.

8.4.5 Training and Competence Management

Training and competency management involve identifying the essential skills employees need to achieve performance targets within their specific roles. This process includes developing these skills to align with the organization's operational strategy.

Cyber exercises simulate potential cyber incidents to construct hypothetical scenarios for evaluating impact and recovery strategies. The primary objective of these activities is to strengthen an organization's operational effectiveness and response readiness during major data security breaches, while also reducing and controlling the consequences of real-world cyberattacks. (Traficom, 2024)

Live, Virtual, Constructive (LVC) training is an integrated and immersive environment that combines real-world resources (live), human-operated simulators (virtual), and computer-generated entities (constructive). This approach improves an organization's operational readiness by providing cost-effective and realistic training for complex, multidisciplinary situations.

8.4.6 Continuous Improvement

Continuous improvement involves regularly assessing and enhancing the effectiveness of an organization's cybersecurity solutions and processes. This must approach as a systematic, long-term, and goal-driven endeavour. These activities should aim to foster a culture of ongoing improvement.

Continuous improvement relies on strategic management and adaptability. This includes fully understanding log analysis and relevant data, assessing impacts carefully, analysing situations thoroughly, incorporating feedback effectively, and updating systems promptly. Detailed documentation of incidents and recovery phases is essential to support actions, foster trust, and maintain transparent communication in continuity management. (Lehto and Pöyhönen, 2026)

9 Future Developing Maritime Cybersecurity

9.1 Threat Environment is Changing

Mosaic Warfare is a US defence strategy developed by DARPA that combines numerous low-cost, distributed, and unmanned systems in different domains (air, sea, land, space, information, cyber) to form a complex and flexible "mosaic". An approach based on artificial intelligence-based, agile, and distributed autonomous units produces superiority precisely through controlled complexity and different platforms. (Jasper & Hollingshead, 2022)

The key advantage of Mosaic Warfare's asymmetric approach is its ability to add highly effective and unexpected elements to the battlefield, which now includes unmanned autonomous and semi-autonomous platforms on land, at sea (surface and subsurface), and in the air. In addition to these physical platforms, defensive and offensive autonomous and semi-autonomous cyber tools are used.

The speed of recent developments requires leaders and system developers to understand the future of autonomous warfare. In the future, various platforms will be autonomous, guiding themselves, identifying, tracking and engaging targets independently. In addition to the autonomy of physical platforms, C5ISR systems process and analyse signals, observations and other intelligence information at a remarkable speed. This enables faster detection, situational awareness, decision-making and response.

Developing future maritime cybersecurity focuses on securing increasingly automated, AI-driven, and connected shipping infrastructure against sophisticated threats.

9.2 Artificial Intelligence and Autonomy

Conflict in cyberspace is constant, low-cost and uninhibited by traditional definitions of territory and country. Now, developers are taking cyber capabilities one step further, using developments in artificial intelligence and machine learning to create autonomous weapons.

Today, technical limitations prevent implementations of deep neural networks and machine learning from reaching high levels of intelligence. Complex tasks such as natural language processing or understanding the breadth and depth of human emotions remain difficult. With the development of quantum computing, this situation is changing.

Anthropic company introduced its advanced AI model, Mythos, in spring 2026. The company claims Mythos can radically improve both offensive and defensive cyber operations by excelling beyond humans at certain hacking and cybersecurity tasks. According to Anthropic, the tool has already discovered thousands of critical vulnerabilities, including some that have existed for years in prominent operating systems and web browsers. Nonetheless, experts argue that Mythos represents a step forward rather than a groundbreaking change, noting that other AI tools can also detect zero-day vulnerabilities. (Milmo, Makortoff and Down, 2026)

Mythos can autonomously create exploit chains, carry out attacks, and hide its actions. While it offers benefits for cybersecurity defence, its dual-use nature means it could be exploited by malicious actors for cyber intelligence or damaging critical infrastructure. (McMahon and Tidy, 2026)

9.3 Digital Convergence

Digital convergence is merging distinct technologies, with the aim of achieving performance and efficiency in cyberspace. Digital convergence is needed to advance maritime cybersecurity. Consistent, rapid and scalable impacts across multiple domains will be crucial to the future of cybersecurity. Seamless integration of full-spectrum cyber (offensive and defensive cyber), electronic warfare, information warfare and space-based capabilities will provide the necessary capability to defend against a variety of threats. (Coleman, 2025)

Military digital convergence refers to the rapid integration of sensors, weapons systems, and command networks into a unified digital ecosystem, leveraging artificial intelligence and data fusion to increase mission autonomy and superiority in cyberspace. Military digital convergence enables the shrinking of platforms and the improvement of their capabilities and adaptability to achieve mission autonomy. (Bratton, 2019)

To achieve convergence, security strategies must shift from isolated, standalone products to integrated and AI-driven approaches. By merging domains, vulnerabilities at their intersections are reduced. Advanced cybersecurity systems offer a comprehensive perspective on overall risks. Looking ahead, proactive monitoring and rapid alerts in cyberspace will be essential for swiftly identifying and reacting to security threats.

Looking ahead, proactive monitoring and rapid alerts in cyberspace will be essential for swiftly identifying and reacting to security threats.

9.4 Harbour Digitalization

Harbor digitalization involves adopting technologies like AI, IoT, and automated systems to optimize port operations, improve efficiency, and reduce emissions. Key solutions include Port Community Systems (PCS), automated container handling, and digital twins for real-time tracking of vessels and cargo. This transformation aims for paperless, sustainable trade and enables smart, autonomous shipping. Smart ports play a central role in future transport logistics and supply chains. Digitalization helps improve the efficiency of terminal systems in the processes of these ports. In the best cases, digitalization can also promote the reduction of emissions by optimizing port operations and enhancing cargo and people flows while improving the experience for all stakeholders. (Pöyhönen and Lehto, 2023)

Innovative technology plays a key role in the digitalization of ports. It aims to optimize the efficiency of port operations. Optimization of efficiency aims to achieve short ship turnaround and berthing times, smooth port processes and reduce carbon dioxide emissions in ports with the goal of carbon neutrality.

9.5 Autonomous Ships

Autonomous ships (Maritime Autonomous Surface Ships - MASS) are vessels operating with varying degrees of automation, from remote control to full AI-driven independence, designed to enhance safety, reduce crew costs, and improve fuel efficiency. They use sensors, AI, and machine learning for navigation, with key applications including short-sea shipping and container transport.

Technological innovation within the maritime industry has resulted in rapid developments that will see the commercial use of autonomous ships, whether they are controlled remotely or are fully autonomous. Such change requires robust regulation to ensure safety and security at sea. (IMO, n.d.b.)

IMO aims to integrate new and advancing technologies in its regulatory framework - balancing the benefits derived from new and advancing technologies against safety and security concerns, the impact on the environment and on international trade facilitation, the potential costs to the industry, and their impact on personnel, both on board and ashore. IMO wants to ensure that the regulatory framework for Maritime Autonomous Surface Ships keeps pace with technological developments that are rapidly evolving. In 2021 IMO conducted a regulatory scoping exercise on Maritime Autonomous Surface Ships that was designed to assess existing IMO instruments to see how they might apply to ships that utilize varying degrees of automation. The regulatory scoping exercise (RSE) for safety treaties was finalized at the 103rd Session of the MSC in May 2021, and for treaties under the purview of the Legal Committee, at its 108th session in July 2021. The FAL Committee approved the outcome of the RSE of treaties under its remit at FAL 46 in May 2022. (IMO, n.d.b.)

Cybersecurity in autonomous vessels is crucial to prevent ship hijacking, collisions and environmental disasters. Attention should be paid to protecting artificial intelligence systems, sensors and remote communications. Key threats include GNSS spoofing, sensor bias and system hacking. Security requires robust integration of IT and operational technology (OT) defences. (Sungbaek et.al., 2022)

Because autonomous ships have more interconnected IT and OT systems, creating a broad attack surface, their cybersecurity is much more demanding than that of traditional ships. Attack targets related to autonomous ships include positioning systems, sensors, firmware, voyage data recorders, ship area networks (SANs), communication systems, and remote operating systems. Important cyberattack vectors include malicious code injection, firmware updates, tampering with ship network packets, USB attacks, spoofing of Global Navigation Satellite System (GNSS) and Automatic Identification System (AIS), jamming, and interception of ship-to-shore control centre (SCC) communications. (Yousaf et.al., 2024)

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) describes nine threat categories against autonomous vessels:

- Attacks to disrupt radio frequency signals
- Attacks to deceive or degrade sensors
- Attacks to intercept or modify communications
- Attacks on OT systems
- Attacks on IT systems
- Attacks on AI systems
- Attacks through supply chains
- Attacks through physical access
- Attacks on Shore Control Centre
- (Yousaf et.al., 2024)

9.6 Satellite Positioning and Maritime Cybersecurity

Satellite navigation (GNSS) is foundational to modern maritime operations but faces significant cybersecurity threats, with jamming and spoofing incidents increasing by 50% in early 2026. The disruptions target critical GNSS services including GPS, Galileo and GLONASS, enabling attackers to either block signals entirely or manipulate positioning data, with the potential to compromise vessel navigation, safety systems and satellite connectivity. Recent observations show that disruptions are no longer isolated incidents. They are becoming a permanent phenomenon on major sea routes, requiring operators to adopt a more flexible and diverse approach to navigation and communication links. (Ribeiro, 2026)

Modern vessels rely heavily on satellite-based navigation and timing systems for:

- ECDIS navigation and route planning.
- Collision avoidance and traffic separation schemes.
- Port approach and berthing operations.
- Dynamic positioning systems.
- Cargo timing and logistics coordination.

GNSS spoofing occurs when attackers transmit counterfeit satellite signals that override legitimate ones, causing navigation systems to calculate false positions or headings. Unlike GNSS jamming, which results in signal loss,

spoofing is more dangerous because systems continue operating with incorrect data. The maritime security threat posed by GNSS spoofing is that it often bypasses traditional defences. Attacks do not install malware, do not necessarily compromise the network, and do not trigger alerts from IT security tools. In such cases, navigation systems may function "normally" even if they provide false information. (Crawford, 2025)

GPS spoofing countermeasures involve detecting, flagging, and mitigating forged GNSS signals to prevent navigation errors. Key strategies include signal monitoring (strength, time-of-arrival), cryptographic authentication, using multi-band/dual-polarized antennas, and integrating inertial navigation systems (INS) to detect inconsistencies. GNSS spoofing has transformed navigation from a purely operational concern into a cybersecurity priority. In GNSS-obstructed and free conditions, inertial navigation systems with a north-facing gyrocompass are available to maintain reliable navigation in such difficult conditions. MEMS (micro-electromechanical systems) is the technology of microscopic devices incorporating both electronic and moving parts. GNSS-assisted INS implemented using MEMS technology provide highly accurate positioning, velocity, acceleration and heading even in the most demanding conditions. MEMS systems detect pitch, roll and yaw. Accessories are available for the multiband GNSS receiver, which increases its resistance to GNSS jamming and spoofing. (Brown, 2024)

9.7 Maritime Cybersecurity Strategy Management

Developing maritime cybersecurity requires implementing robust and proactive strategies to protect ships and port infrastructure from growing digital threats, often driven by new mandatory regulations. Key areas of focus include creating an advanced cyber situational picture, conducting mandatory assessments required by regulation, organizing regular cyber exercises, and utilizing artificial intelligence to detect threats and secure ships and port operations.

A robust maritime cybersecurity strategy integrates IT and OT security to protect ships, ports and cargo from digital threats in line with IMO and IACS UR E26/E27 regulations. It focuses on network segmentation, risk assessment, employee training and incident response to ensure operational resilience and security. (IMO, 2025; BIMCO et.al. 2024; IAPH, 2021)

Key pillars of a maritime cybersecurity strategy are:

1. **Risk management and compliance:** Adopting a holistic risk management approach is crucial, as required by IMO MSC.428(98) to include cyber risk in safety management systems. Key provisions include the EU NIS2 and the new IACS standards for ship systems.
2. **Network segmentation:** Separating critical operational systems on ships and in ports from non-critical systems is essential. In addition, effective identity and access management for segmented systems is required.
3. **OT and IT Security:** Protecting the various systems of ship ports according to their specific characteristics, utilizing the latest cybersecurity technologies
4. **Operational Resilience:** Developing comprehensive and up-to-date data breach response plans to minimize downtime and costs caused by data breaches and ensure rapid recovery.
5. **Training and Human Factors:** Regular cybersecurity training for port operators and ship crew and staff is vital.
6. **Asset Management and Patching:** Maintaining an inventory of all networked devices in ports and ships and regularly patching systems to address vulnerabilities.

(IMO, 2025; BIMCO et.al. 2024; IAPH, 2021)

10 Conclusion

Many maritime networks still use legacy technologies that were not originally designed to connect to the internet. These complex networks span both information technology (IT) and operational technology (OT) systems, creating vulnerabilities that hackers or state actors can exploit. In the past, air-gaps – physically isolating protected networks from unprotected ones – were a common security measure. However, modern ships have become highly networked, making it easier for malicious actors to penetrate critical systems by exploiting simple technological methods or human weaknesses created by users. The same connectivity challenge applies to ports and port operations.

To effectively tackle cyber risks in the maritime environment, a comprehensive and multilayered approach needs to be implemented by the maritime stakeholders to integrate technical, procedural, and organizational measures.

The maritime sector uses a comprehensive cyber risk management plan to defend itself against the growing risks of cyberattacks. It is based on continuous monitoring and strong cybersecurity measures to protect critical infrastructure and sensitive data on board ships and in ports. It is important to integrate cybersecurity into governance and compliance; conduct regular cyber risk assessments to anticipate and assess threats. Assess the likelihood and impact and prioritize risks and improve cybersecurity awareness, and provide mandatory cybersecurity training for crew members, port staff and IT/OT users. Incident response plans should be developed and tested, and regular cybersecurity exercises should be conducted on board ships and port terminals. By focusing on proactive risk management and encouraging teamwork and information sharing, the maritime sector is striving to improve its ability to resist cyber threats and keep maritime operations safe, secure and reliable as technology advances. (Zhou, 2025)

Organizations should implement automated security and continuous monitoring to provide sustained system visibility. During the continuous operations phase, organizations should use real-time dashboards and alert mechanisms to provide immediate threat detection and rapid response.

Maritime is currently undergoing a profound digital transformation. Technologies such as artificial intelligence, autonomy and quantum are redefining the way maritime transport is conducted. New technologies also bring new risks.

Autonomous surface vessels are already being tested for short-haul cargo transport, offshore inspection and surveillance. There is growing commercial appeal for systems such as assisted navigation, autonomous docking and smart maintenance platforms – technologies designed to reduce human error and increase operational efficiency. Full autonomy on ocean-going vessels is still a relatively distant goal. Until then, hybrid autonomy is used, in which human operators and intelligent systems work together to make maritime navigation safer, more efficient and more predictable. This human-machine collaboration allows for the validation of technologies, the building of operational trust and incremental progress – without compromising safety or accountability. Current AI systems can reliably handle narrow, well-defined tasks – such as collision avoidance, engine diagnostics or port manoeuvres – especially in controlled environments such as ports or inland waterways. However, operations on the high seas still pose significant challenges: extreme weather conditions, limited connectivity, system malfunctions and the unpredictable nature of sea conditions require constant human supervision. (Zissis, 2025)

As autonomy expands, special attention must be paid to the reliability, responsibility and fault tolerance of systems. How they function in difficult conditions, for example in various cyber threat situations. In addition to security solutions, it is necessary to take care of regulation in the sector and maintain trust in the latest technologies. (Zissis, 2025)

ANNEX 1
– Cybersecurity regulations, standards and instructions

1. REGULATIONS AND STANDARDS

IAPH: Cybersecurity Guidelines for Ports and Port Facilities, 2021
Released in July 2021, version 1.0 provides a comprehensive, executive-level framework for managing cyber risks in the maritime sector.

IMO: Guidelines on Maritime Cyber Risk Management, 2025
The IMO's updated 4 April 2025 Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.3) provide a crucial, updated framework for identifying, protecting against, detecting, responding to, and recovering from cyber threats. The guidelines require integrating cyber risks into safety management systems (SMS) in compliance with the ISM Code. Key focus areas include securing IT/OT networks, training, and mitigating risks from increasing automation.

USCG: Final Rule on Cybersecurity in the Marine Transportation System, 2025
The US Coast Guard Final Rule on "Cybersecurity in the Marine Transportation System," published January 17, 2025, mandates stringent cybersecurity measures for U.S.-flagged vessels, OCS facilities, and MTSA-regulated facilities, effective July 16, 2025.

IMO Resolution MSC.428(98), 2017
IMO Resolution MSC.428(98) adopted in 2017, mandates that maritime cyber risks be addressed within safety management systems (SMS), effective from the first annual compliance verification after January 1, 2021. It identifies an urgent need to raise awareness on cyber risks, threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks. Thus, all maritime stakeholders should work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities. The resolution furthermore affirms that the SMS should consider cyber risk management in accordance with the objectives and functional requirements of the ISM Code. In combination with this resolution, IMO also released Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3). This provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes.

BIMCO et.al.: The Guidelines on Cyber Security Onboard Ships Version 5, 2024
The purpose of these guidelines is to improve the safety and security of seafarers, the environment, the cargo and the ships. The guidelines aim to assist in the development of a proper cyber risk management strategy in accordance with relevant regulations and best practises on board a ship with a focus on work processes, equipment, training, incident response and recovery management.

IACS, new unified requirements (URs) for cyber security, 2024
International Association of Classification Societies' (IACS) new unified requirements (URs) for cyber security taking effect from 1 July 2024, this obliges owners, yards and suppliers to build cyber security barriers into their systems and vessels, requiring compliance across the full spectrum of critical on-board control and navigation systems.
The IACS URs for cyber security consist of two sets of rules: E26 governs system integration, while UR E27 applies to essential onboard systems. Both must be met by vendors and yards and will be mandatory for all newbuilds with contracts signed after 1 July 2024.
The URs (maritime cyber security regulations) will apply to everything computer-based on board such as main-engine control systems, steering, cooling systems, fire detection, communications systems including public address systems, and navigation systems – anything that is integral to making the ship move, navigate and operate safely.
The URs are minimum prescriptive requirements agreed by all IACS members. Based on the IEC 62443 standards that address OT cyber security in a holistic way, they aim to ensure the secure integration of both OT and IT equipment into the vessel's network during the design, construction, commissioning and operational life of the ship, covering equipment identification, protection, attack detection, response and recovery. These regulations also aim to ensure system integrity is secured and hardened by third-party equipment suppliers.

EU Directive on Network and Information Systems (NIS2), 2024
Set to be implemented in October 2024, this obliges EU member states to adopt cyber security strategies and establish competent cyber security structures across their jurisdictions. The directive will ensure that operators of essential services, including major ports, shipping companies and even single vessels like FSRUs, take appropriate security measures and report serious cyber incidents.
As the maritime industry continues to modernize, cybersecurity will remain a top concern. Emerging technologies like blockchain for secure transactions, AI-driven threat detection, and quantum-safe encryption are expected to play a crucial role in strengthening cybersecurity defences. While new regulations and best practices set a strong foundation, ongoing vigilance, collaboration, and investment in cyber resilience will be essential to safeguarding the future of shipping against evolving cyber threats.

ISO/IEC 27001 for Maritime Cybersecurity, 2022
Information security, cybersecurity and privacy protection — Information security management systems — Requirements, Edition 3, 2022.

IEC 60945, 2002
It is the international standard for maritime navigation and radio communication equipment, specifying minimum performance requirements, testing methods, and required results. It ensures equipment reliability regarding electromagnetic compatibility (EMC) and environmental factors (saltwater, vibration, temperature) in harsh marine environments.

IEC 60533, 2015
It is the international standard for electromagnetic compatibility (EMC) of electrical/electronic equipment on ships with metallic hulls. It defines minimum emission, immunity, and performance requirements to ensure systems function safely without interfering with each other, supporting SOLAS 74 requirements. The current Edition 3.0 covers testing methods and mitigation techniques like bonding.

IEC 60092 series, 2005
It provides international standards for electrical installations on ships and fixed/mobile offshore units, ensuring safety, reliability, and performance in marine environments.

2. INSTRUCTIONS AND REPORTS

ENISA: Port Cybersecurity - Good practices for cybersecurity in the maritime sector, 2019
This report identifies challenges, in relation to critical operations, stakeholder's ecosystem and assets identification. It then lists the main threats posing risks to the port ecosystem and describes key cyberattack scenarios that could impact them.

ENISA: Cyber Risk Management for Ports - Guidelines for cybersecurity in the maritime sector, 2020
This report aims to provide port operators with good practices for cyber risk assessment so that they can adapt to whatever risk assessment methodology they follow.

Finnish National Emergency Supply Organization, the Maritime Transport Pool: Maritime Cybersecurity – Best Practices for Vessels, 2021
This report is the result of a study commissioned by the Finnish Shipowners' Association and the Finnish Security and Defence Council to map the cybersecurity situation in the Finnish maritime sector. Deductive Labs Oy was selected as the project implementer. This document proposes and presents the different phases and best practices for cybersecurity of ships.

Supreme: Cybersecurity in Shipping: New Standards and Best Practices for 2025:
https://supremefreight.com/cybersecurity-in-shipping-new-standards-and-best-practices-for-2025/

DNV: Maritime cybersecurity:
https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/regulations/

REFERENCES

Akpan F., Bendiab G., Shiaeles S., Karamperidis S. and Michaloliakos M. 2022. Cybersecurity Challenges in the Maritime Sector, Network 2022, 2, 123–138. https://doi.org/10.3390/network2010009

Ashenden D. 2011. Cyber Security: Time for Engagement and Debate, Proceedings of the 10th European Conference on Information Warfare and Security, the Institute of Cybernetics at the Tallinn University of Technology Tallinn, Estonia, 7-8 July 2011.

Bertino E., Martino L.D., Paci F., and Squicciarini A.C. 2010. Web services threats, vulnerabilities, and countermeasures in Security for Web Services and Service-Oriented Architectures, pp. 25–44. Springer.

BIMCO et.al. 2017. The guidelines on Cyber Security Onboard Ships, version 2, December 2017.

BIMCO et.al. 2018. The Guidelines on Cyber Security Onboard Ships, Version 3, December 2018.

BIMCO et.al. 2021. The Guidelines on Cyber Security Onboard Ships, Version 4, December 2021

BIMCO et.al. 2024. The Guidelines on Cyber Security Onboard Ships, Version 5, December 2024.

Bratton J. 2019. The Military Digital Convergence, Mercury blog, March 5, 2019, https://www.mrcy.com/company/blogs/military-digital-convergence

Bronk C. and deWitte P. 2022. Maritime Cybersecurity: Meeting Threats to Globalization's Great Conveyor in Martti Lehto and Pekka Neittaanmäki, eds., Cyber Security: Critical Infrastructure Protection (Barcelona, Springer 2022).

Brown J. 2024. What is GPS Spoofing? ...And How to Avoid It, blog in Aircraft Performance Group, Apr 29, 2024, https://flyapg.com/blog/what-is-gps-spoofing#:~:text=Some%20entities%20that%20may%20carry%20out%20GPS,sources%20*%20Crowd%2Dsourced%20detection%20*%20Cryptographic%20authentication

C4ADS. 2019. Above Us Only Stars – Exposing GPS Spoofing in Russia and Syria, March 26, 2019, https://c4ads.org/reports/above-us-only-stars/

Chong J. 2013. Why is our cybersecurity so insecure? New Republic, https://newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure

Coleman B. 2025. Embracing Full-Spectrum Cyber, Signal Sep 15, 2025.

Constantin L. 2021. 33 hardware and firmware vulnerabilities: A guide to the threats. CSO, https://www.csoonline.com/article/3410046/hardware-and-firmware-vulnerabilities-a-guide-to-the-threats.html

Crawford C. 2025. GPS Spoofing Threats Disrupting Maritime Navigation, blog, December 16, 2025, https://saturnpartners.com/2025/12/gps-spoofing-maritime-cybersecurity/

Cutlip K. 2016. Spoofing: One Identity Shared by Multiple Vessels, GFW blog, https://globalfishingwatch.org/data/spoofing-one-identity-shared-by-multiple-vessels/

Darktrace. n.d. What is Maritime Cybersecurity? https://www.darktrace.com/cyber-ai-glossary/cybersecurity-in-maritime

deWitte P. and Lehto M. 2025. Maritime Transportation System and Cyber Threats in Demchak C. and Tangredi S. Cyber Warfare and Navies, U.S. Naval War College 2025. ISBN 978-1-68247-585-0

DHS. 2014. Sector risk snapshots. U.S. Department of Homeland Security. DHS Science and Technology website, 1 January 2015, https://www.dhs.gov/science-and-technology/2014-snapshot-archives

Dunn Cavelty, M. 2010. The Reality and Future of Cyberwar, Parliamentary Brief, 30th March 2010, www.parliamentarybrief.com/2010/03/the-reality-and-future-of-cyberwar

ENISA. 2015. Cyber security and resilience of intelligent public transport: Good practices and recommendations. European Union Agency for Network and Information Security (ENISA).

ENISA. 2019. Port Cybersecurity - Good practices for cybersecurity in the maritime sector, November 2019

ENISA. 2020. Cyber Risk Management for Ports - Guidelines for cybersecurity in the maritime sector, December 2020.

FCC. 2014. Cyber security planning guide. Federal Communications Commission (FCC).

Forbes V. 2018. The Global Maritime Industry Remains Unprepared for Future Cybersecurity Challenges, Future Directions, 21 August 2018, http://www.futuredirections.org.au/publication/the-global-maritime-industry-remains-unprepared-for-future-cybersecurity-challenges/

Gronholt-Pedersen J. 2017. Maersk says global IT breakdown caused by cyber-attack, Reuters, https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19I1NO

HVK. 2021. Maritime Cybersecurity Report – Finnish Maritime Cybersecurity Maturity.

IET. 2020. Cyber Security for Ports and Port System – Good Practice Guide, Institution of Engineering and Technology, London, United Kingdom

IMO. n.d.a. Maritime Domain Awareness, https://www.imo.org/en/ourwork/security/pages/maritime-domain-awareness.aspx

IMO, n.d.b. Autonomous shipping, https://www.imo.org/en/mediacentre/hottopics/pages/autonomous-shipping.aspx#:~:text=Technological%20innovation%20within%20the%20maritime%20industry%20is,on%20board%20and%20of%20the%20vessel%20itself.

IMO. 2017a. Maritime cyber risk, June 2017. http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/cyber-security.aspx

IMO. 2017b. Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3, 5 July 2017. https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf

IMO. 2025. Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3/Rev.3 4 April 2025. https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/FAL%20related%20nonmandatory%20documents/MSC-FAL.1-Circ.3-Rev.3.pdf

Jasper S. and Hollingshead T. 2022. Mosaic Warfare Networks Can Serve Naval Expeditionary Forces, Signal Jan 01, 2022.

Johnson B. 2022. Maritime Cyber Incidents Increased at Least 68 Percent in 2021, Coast Guard Reports, Government Technology and Service Coalition (GTSC) Homeland Security Today, 26 August 2022, https://www.hstoday.us/featured/maritime-cyber-incidents-increased-at-least-68-percent-in-2021-coast-guard-reports/.

Karamperidis S. Kapalidis C. and Watson T. 2021. Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches, J. Mar. Sci. Eng. 2021, 9, 1323. https://doi.org/10.3390/jmse9121323

Kessler G. 2019 Cybersecurity in the Maritime Domain, U.S. Coast Guard, Proceedings of the Marine Safety & Security Council 76, no. 1(Spring 2019): 34-39, https://commons.erau.edu/cgi/viewcontent.cgi?article=2377&context=publication;

Kessler G. and Shepard S. 2022. Maritime Cybersecurity: A Guide for Leaders and Managers, self-published, February 2022.

Kott A., Linkov I. 2019. Cyber Resilience of Systems and Networks, in Risk, Systems and Decisions, Springer.

Kovanen T., Nuojua V., Lehto M. 2018. Cyber Threat Landscape in Energy Sector, the 13th International Conference on Cyber Warfare and Security, 8 - 9th March 2018, National Defense University, Washington DC, USA, pages 353-361.

Kovanen T., Pöyhönen J., Lehto M. 2021a. Cyber Threat Analysis in the Remote Pilotage System. 20th European Conference on Cyber Warfare and Security, 24th - 25th June 2021, Chester, UK, pages 221-229.

Kovanen T., Pöyhönen J., Lehto M. 2021b. ePilotage System of Systems' Cyber Threat Impact Evaluation, 16th International Conference on Cyber Warfare and Security, 25th – 26th February 2021, Tennessee, USA, pages 144-151.

KRUGER. 2025. What are the key components of a marine safety system on vessels? PAT-Kruger marketing, https://www.pat-kruger.com/what-are-the-key-components-of-a-marine-safety-system-on-vessels/

Larsen M. and Lund M. 2021. Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review, IEEE Access, Volume: 9, page(s): 144895 – 144905, 25 October 2021. DOI: 10.1109/ACCESS.2021.3122433

Lehto M. 2013. The Cyberspace threats and cyber security objectives in the Cyber Security Strategies. International Journal of Cyber Warfare and Terrorism, Vol. 3, Issue. 3, pages 1-18.

Lehto M. 2020. Cyber Security in Aviation, Maritime and Automotive, in Pedro Diez, Pekka Neittaanmäki, Jacques Periaux, Tero Tuovinen, Jordi Pons-Prats (Edit.) Computation and Big Data for Transport, in series Computation Methods in Applied Sciences, Springer 2020, pages 19-32. https://doi.org/10.1007/978-3-030-37752-6_2

Lehto M. and Pöyhönen J. 2026. Comprehensive cyber security and resilience architecture framework, in Lehto M. & Neittaanmäki P. (Edit.) Cyber Security - Policy and Technology, Springer 2026, pages 287-337. ISBN 978-3-032-08890-1

Loomis W., Singh V. V., Kessler G., and Bellekens X. 2021. Raising The Colors: Signaling for Cooperation on Maritime Cybersecurity, Atlantic Council, October 2021.

Maure D. 2018. The Logistics of a Port, Shipping & Logistics Blog, March 22, 2018. https://www.shiplilly.com/blog/the-logistics-of-a-port/

McMahon L. and Tidy J. 2026. What is Claude Mythos and what risks does it pose? BBC, 17.4.2026, https://www.bbc.com/news/articles/crk1py1jgzko

Meland P.H., Bernsmed K., Wille E., Rødseth Ø.J. & Nesheim D.A. 2021. A Retrospective Analysis of Maritime Cyber Security Incidents, the International Journal on Marine Navigation and Safety of Sea Transportation Volume 15 Number 3 September 2021 DOI: 10.12716/1001.15.03.04.

Milmo D., Makortoff K. and Down A. 2026. What is Mythos AI and why could it be a threat to global cybersecurity? Guardian, 22.4.2026, https://www.theguardian.com/technology/2026/apr/22/what-is-anthropic-mythos-ai-threat-global-cybersecurity

MITAGS. 2024. Guide to Ship Cybersecurity, blog, last updated on Mar 14, 2024, https://www.mitags.org/guide-ship-cybersecurity/

Oceum. 2026. Ship Machinery Systems: Practical Engineering Guide from Real Operations. https://oceum.com.br/ship-machinery-systems/

Pijpker J. and McCombie S. 2026. How Did They get Aboard my Ship? Analysing Vessel Cyber Incidents Using the Cyber Kill Chain. The Proceedings of the 21st International Conference on Cyber Warfare and Security, 5-6 March 2026, University of North Carolina, Wilmington, USA, pages 374-382.

Pöyhönen J. 2020. Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa. Systeemiajattelu. JYU dissertations 270.

Pöyhönen J., Hummelholm A., Lehto M. 2022. Cybersecurity risk assessment subjects in information flows. 21st European Conference on Cyber Warfare and Security, 16th – 17th June 2022, Chester, UK, pages 222-230.

Pöyhönen J. and Lehto M. 2023. Comprehensive cyber security for port and harbor ecosystems, in Frontiers in Computer Science, 25 October 2023, DOI: 10.3389/fcomp.2023.1154069.

Pöyhönen J., Simola J., Irfan K., Lehto M., Wali S. 2023. Assessment of cyber security risks – Smart terminal process, 22nd European Conference on Cyber Warfare and Security, 22 - 23 June 2023, Athens, Greece, pages 366-373.

Ribeiro A. 2026. Marlink warns surge in satellite spoofing is blinding maritime digital infrastructure, disrupting vessel navigation, blog, March 26, 2026, https://industrialcyber.co/transport/marlink-warns-surge-in-satellite-spoofing-is-blinding-maritime-digital-infrastructure-disrupting-vessel-navigation/#:~:text=New%20data%20from%20Marlink%20reports%20a%2050%25,incidents%20affecting%20global%20shipping%20in%20March%202026%2C

Rodrigue J-P. and Notteboom T. 2020. Port Terminals, in Jean-Paul Rodrigue (Edit.) The Geography of Transport Systems, New York: Routledge, pages 366-373. ISBN 978-0-367-36463-2.

Rodrigue J-P. and Slack B. 2020. The Function of Transport Terminals in Jean-Paul Rodrigue (Edit.) The Geography of Transport Systems, New York: Routledge. ISBN 978-0-367-36463-2.

Safety4Sea. 2018. 2018 highlights: Major cyber-attacks reported in maritime industry. Safety4Sea, https://safety4sea.com/cm-2018-highlights-major-cyber-attacks-reported-in-maritime-industry/

Securewest. 2026. Why Legacy Ship Systems Are a Growing Cyber Risk in 2025 – And What to Do About It, blog, January 20, 2026 https://www.securewest.com/news/maritime/why-legacy-ship-systems-are-a-growing-cyber-risk-in-2 025-and-what-to-do-about-it/

Securicon. 2019. What's the difference between OT, ICS, SCADA and DCS? Securicon, Alexandria, VA, https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/

Simola J. and Pöyhönen J. 2022 Emerging Cyber risk Challenges in Maritime Transportation. Proceedings of the 17th International Conference on Information Warfare and Security, 2022, pages 306-314.

Simola J., Pöyhönen J., Lehto M. 2023. Cyber Threat Analysis in Smart Terminal Systems, 18th International Conference on Cyber Warfare and Security, 9th -10th March 2023, Towson University, Maryland USA, pages 369-378.

Sungbaek C., Erwin O., Gabor V. and Vasco P. 2022. Cybersecurity Considerations in Autonomous Ships, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) report, https://ccdcoe.org/uploads/2022/09/Cybersecurity_Considerations_in_Autonomous_Ships.pdf

Thai V. V. and Grewal D. 2007. The Maritime Security Management System: Perceptions of the International Shipping Community, Maritime Economics & Logistics 9(2):119-137, June 2007. DOI:10.1057/palgrave.mel.9100175.

Traficom. 2024. Exercises, https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/exercises

Weed A.S. 2017. US policy response to cyber-attack on SCADA systems supporting critical national infrastructure. Air University Press.

Yousaf A., Amro A., Kwa P., Li M. and Zhou J. 2024. Cyber risk assessment of cyber-enabled autonomous cargo vessel, International Journal of Critical Infrastructure Protection, Volume 46, September 2024, https://doi.org/10.1016/j.ijcip.2024.100695Get rights and content

Zhou J. 2025. Maritime Cybersecurity: A Big Change Ahead, IEEE Security & Privacy, Jul.-Aug. 2025, pp. 4-7, vol. 23. DOI Bookmark: 10.1109/MSEC.2025.3589068

Zissis D. The future of the shipping industry: AI, robotics, and the path to autonomy, University of the Aegean, October 16, 2025, https://28digital.eu/newsroom/grow-digital-insights/the-future-of-the-shipping-industry-ai-robotics-and-the-path-to-autonomy/

Our Aim is to Add
Cyber Capabilities
in the World

Contact

Cyberwatch Oy | Kansakoulukatu 1b | 00100 Helsinki, Finland
aapo@cyberwatchfinland.fi | info@cyberwatchfinland.fi | +358 40 500 8177