European Commission

Critical Maritime Routes Programme Monitoring, Support and Evaluation Mechanism (CRIMSON III)

Cybersecurity in Maritime Critical Infrastructure

Reflection on African Ports

Service for Foreign Policy Instruments

EUROPEAN COMMISSION
EuropeAid Co-operation Office
Instrument for Stability/ Contract no. No. IFS/2019/410-525

Submitted to:
Ondrej Vosatka
Service for Foreign Policy Instruments (FPI)
FPI.1 – Peace and Stability – Global and Transregional Threats and Challenges
EEAS 02/9A Rond Point Schuman, Brussels

Contract no. No. IFS/2019/410-525

Date: 20/04/2023

Authors:
Nineta Polemi, Cybersecurity professor, dpolemi@gmail.com
Christophe Van Maele, Maritime expert, cvanmaele@portconsult.eu

The work was coordinated by Evelyn Vancollie, CRIMSON Project Coordinator.

This study is funded by the Service for Foreign Policy Instrument (FPI) of the European Union through the Critical Maritime Routes Monitoring, Support and Evaluation Mechanism (CRIMSON III), implemented by RUSI Europe. It was supported by EU CyberNet.

This report has been produced with the assistance of the EU. The contents of this report are the sole responsibility of the authors and can in no way be taken to reflect the views of the EU.

Table of Contents

List of Acronyms

AI	Artificial Intelligence
AIS	Automatic Identification System
CCTV system	Closed Circuit Television
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CISO	Chief Information Security Officer
COP	Code of Practice
COSCO	China Ocean Shipping Company
CSA	Cyber Security Assessment
CSI	Container Security Initiative
CSIRT	Computer Security Incident Response Team
CSO	Company Security Officer
CSP	Cyber Security Plan
CYSO	Cyber Security Officer
DA	Designated Authorities
DDoS	(Distributed) Denial of Service
DSP	Digital Service Providers
ECDIS	Electronic Chart Display and Information System
EEAS	European External Action Service
EMSA	European Maritime Safety Agency
ENISA	European Union Agency for Cyber Security
EUMSS	European Maritime Security Strategy
GDPR	General Data Protection Regulation
GMDSS	Global Maritime Distress and Safety System
GMN	Global MTCC Network
IACS	International Association of Classification Societies
IAPH	International Association of Ports and Harbors
IBC code	International Code for the Construction and Equipment of Ships carrying Dangerous Chemicals in Bulk
ICS	Industrial Control System
ICT	Information Communication Technology
ILO	International Labour Organization
IMDG Code	International Maritime Dangerous Goods code
IMO	International Maritime Organization
IMSBC code	International Maritime Solid Bulk Cargoes code
IoT	Internet of Things
ISAC	Information Sharing and Analysis Centre
ISM	International Safety Management
ISMS	Information Security Management System
ISPS	International Ship and Port Facility Security
IT	Information Technology
LNG	Liquified Natural Gas
MCS	Mediterranean Shipping Company
MTCC	Maritime Technology Cooperation Centre

NIS	Network and Information Systems
NLF	New Legislative Framework
OES	Operators providing Essential Services
OT	Operational Technology
PCS	Port Community System
PFSO – PSO	Port (Facility) Security Officer
PSA – PFSA	Port (Facility) Security Assessment
PSC	Port State Control
PSO - PFSO	Port (Facility) Security Officer
PSP – PFSP	Port (Facility) Security Plan
RA	Risk Assessment
RIB	Rigid Inflatable Boat
RM	Risk Management
RMF	Risk Management Framework
SCSO	Ship Cyber Security Officer
Security Level 1	ISPS Security Level 1, minimum appropriate protective measures
Security Level 2	ISPS Security Level 2, additional protective security measures, maintained for a period of time as a result of heightened risk of a security incident.
Security Level 3	ISPS Security Level 3, further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent
SeMS	Security Management System
SMS	Safety Management System
SOC	Security Operations Centre
SOLAS	Safety Of Life at Sea
SOP	Standard Operating Procedures
SSO	Ship Security Officer
SSP	Ship Security Plan
STCW	Seafarers' Training, Certification and Watchkeeping
TOS	Terminal Operating System
YARIS	Yaoundé Architecture Regional Information Sharing network

List of Figures

Executive summary

Modern commercial ports are a critical infrastructure which is highly dependent on information systems. The security of a port thus relies on the integrity of both physical and cyber assets. Despite evidence that ports are becoming targets for hackers, whose attacks can affect both cyber and physical assets and halt operations, too many ports have inadequate cybersecurity. Physical threats, incidents, and accidents to the physical assets (e.g., terminals, gates, buildings) of the maritime infrastructures or cyber threats and attacks to the cyber assets (e.g., Port Community Systems, navigation systems) can jeopardise the maritime operations, disrupt supply chains and destroy international trade and commerce.

This desk research provides an assessment of the available maritime security (safety and cybersecurity) concepts for ports as well as security management standards, methodologies, best practices, tools, and frameworks, and analyses the existing legal and regulatory regimes. Furthermore, the report presents cyber threats and attacks that the maritime ecosystem (ports, ships, maritime companies, authorities, maritime supply chains) face due to rapid digitalisation. The consequences and impacts of these threats to the maritime operator, stakeholders, economies, and national safety can be significant. Cybersecurity standards, strategies, legal and policy instruments are presented in this document to serve as examples of efforts to holistically address the maritime cybersecurity challenges. Risk management methodologies, tools and guidelines based on the standards are presented in order to raise awareness of ports of the existing international approaches. Compliance with standards and existing security strategies enhances the resilience of international operations, supply chains and trade.

The report also captures the security awareness level of Sub-Saharan African ports in comparison to European efforts. The two questionnaires in the annexes, developed by the authors, can be distributed to the African maritime stakeholders in order to self-assess the security governance level (Annex A) and their awareness and practices maturity level (Annex B). The questionnaires can also be used to improve their security readiness level. Finally, practical recommendations are made to the EC on how to build better relationships with African ports to raise their security capabilities. The report serves to alert Maritime Ministries and governments of the issues that need to be considered.

The recommendations of the report aim to holistically improve security at African ports, including specific recommendation for cybersecurity. At national level, cybersecurity legislation needs to be reviewed, and senior management at port level should be encouraged to support an investment in security governance, including personnel and resources. Cybersecurity awareness training would be needed for all stakeholders involved and cybersecurity teams should be formed. An inventory of all critical assets, including cyber assets, is recommended, after which a risk assessment can identify cyber threats, risks, and vulnerabilities. Based on these, a cybersecurity management plan can be developed, including the management, response, and recovery of cyber incidents. The suppliers of cybersecurity equipment may have remote access to equipment, and their cybersecurity should also be

assessed. There are existing cybersecurity standards and expertise which can help ports to create and maintain their cyber shield.

There are also recommendations to the EU on how to enhance EU-African collaboration in the areas of maritime security, cybersecurity and the security of supply chains. The EU should seek to build stable collaborations between Ministries of Maritime/Transport, Security Agencies and maritime Information Sharing and Analysis Centres. The EU should also look to close the cyber skills gap with its African partners, including through realistic exercises. Cross-border support in operating maritime Security Operations Centres that will effectively forecast and manage cyber-attacks and security incidents will also enhance collaboration. Harmonising maritime certification efforts will also help, including through joint audits and assessments of the security of the maritime equipment to ensure privacy, security, transparency, interoperability, accountability, liability and compliance international security legislation and guidelines. Finally, there should be regular benchmarks by conducting comparative analysis between ports in the EU, in the Sub-Saharan African region and ports in other regions of the world. This would be useful to highlight successful EU-African security and cybersecurity approaches that can be replicated in other regions.

1 Introduction

The maritime sector sustains societies and economies through the movement of people and vital goods, such as energy (transportation of oil and gas) and food. The economy is critically dependent upon the physical security and safety of the maritime movement of cargo and passengers. However, since maritime activity increasingly relies on Information Communication and Technology (ICT) to optimise its operations (e.g., from navigation to propulsion, from freight management to traffic control communications), cybersecurity has become an essential requirement. Over recent years cyber threats have become a growing menace, spreading across the maritime ecosystem (from ports to maritime companies to other interconnected critical infrastructures, e.g., transport, maritime authorities). Disruption or unavailability of maritime ICT capabilities could potentially, have disastrous consequences therefore, there is an increasing need to ensure physical security and cybersecurity against physical, cyber and hybrid attacks.

In this report, the word security embraces physical security, safety and cybersecurity and needs to be treated holistically, not fragmented since maritime critical infrastructure (CI) includes both physical and cyber assets.

Physical and cyber-security are key challenges at national and international levels. Commercial ports are critical infrastructures (CI) and key economic enablers, thus, their security is essential in the maritime business and one of the greatest marketing advantages in the competitive, fast growing international maritime digital era.

Ports are also indispensable nodes of supply chains involving many strategic stakeholders, business partners and activities interacting with each other. Security and sustainability have emerged as major concerns in ports' supply chains as well. Identifying and managing supply chain threats and their cascading effects and risks are major challenges. The difficulties are partly due to the complexity induced by the large number of related and interdependent activities, processes, entities, and physical and cyber assets in the supply chain. Targeted risk management methodologies and tools to manage physical and cyber-security incidents in the ports and their supply chains are major security challenges.

2 The complex maritime ecosystem

Modern commercial ports, maritime companies and ships are highly dependent on the operation of complex, dynamic ICT systems and ICT-based maritime supply chains and they operate in a complex maritime environment. The maritime environment (figure 1) involves many interacting stakeholders and infrastructures (authorities, ports, maritime and insurance companies, ship-industry, banks, supply chains, other critical infrastructures), as well as assets (physical and cyber).

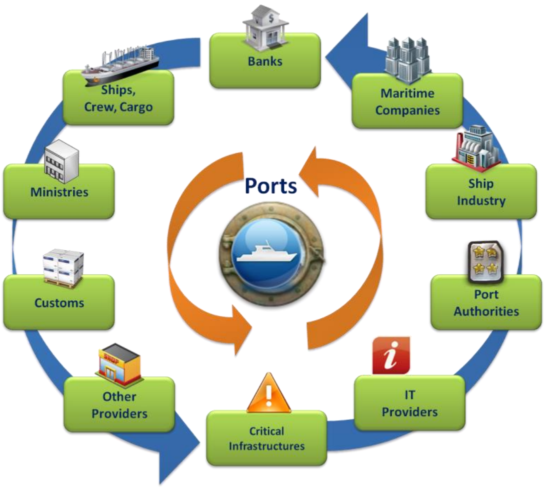


Figure 1 : Maritime Environment[1]

The maritime infrastructures are considered critical according to the NIS and NIS2 Directives (Directives on security of Network and Information Systems)[2] since the interruption of their operations and services would have a negative impact on national, EU and wider international trade as well as occasionally, on human lives.

As Critical Infrastructures, maritime infrastructures are obliged to maintain the security (physical and cyber) of all their assets of their ICT, hosted and operated in their CIs to provide port services. The maritime ICT can be viewed as a physical cyber system with the following six layers:

1. Infrastructure layer (e.g., buildings, platforms, gates, marinas, data centres, terminals, ships)
2. Telecom layer (e.g., networks, telecom equipment, satellites, relay stations, tributary stations);
3. IT layer (e.g., navigation / transmission / monitoring / port community systems, GIS, smart surveillance systems, Internet of Things (IoTs));

[1] (Polemi, 2017)

[2] (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 2016); (Negreiro, 2022)

4. Data (e.g., marine and coastal data, trade data);

5. Maritime Services (e.g., invoicing, navigation, luggage / cargo / vessel / container management, logistics, supply chain services);

6. Users: a. internal users (e.g., operators, administrators, crew); b. external users (e.g., port authorities, maritime companies, customs, insurance companies, IT and supply chain providers); and c. smart objects (e.g., containers, ships, crew cargo, luggage, vehicles).

The first (infrastructure) and sixth (users) are the physical layers of the maritime CIs whereas the layers 2-5 are the cyber layers. The maritime stakeholders need to ensure the confidentiality, integrity, authenticity dimensions of the entire ICT, i.e., the security of the physical assets (safety) and the security of the cyber assets (cybersecurity).

The maritime CIs are of growing economic importance, and they have become a target for hackers, who are increasingly launching physical and cyber-attacks on the ports' and vessels' global navigation systems and cargo management systems. Such attacks can disable a vessel, hijack, divert or steal cargo, while also compromising sensitive customer or corporate data.

Likewise, attacks in the ports' Terminal Operating Systems (TOS), Port Community Systems (PCS) (e.g., supervisory control, SCADA, distributed control systems and programmable logic controllers), or ships' navigation systems may cause disruption or damage to critical mechanical devices (e.g., container cranes, safety and mechanical systems that operate locks and dams), and worse, they may cause loss of life, steal cargo or destroy a ship. An attack on a container TOS could also disrupt intermodal container services involving maritime, rail and truck transportation.

Older port legacy TOS have long service lives and they often operate in independent modes with inadequate password policies and security administration, no data protection mechanisms and protocols that are prone to snooping, interruption and interception which may cause the disruption of various critical port and supply chains operations and services. PCS are complex electronic platforms that connect multiple systems operated by a variety of organisations in the maritime ecosystem and a plethora of ICT providers; PCS security is treated as a cryptographic "black box", where the internal workings are hidden and only inputs and outputs are known.[3] National Single Windows, which are based upon the PCS, need to be assessed and accompanying security policies should guarantee their trustworthy operations.

Unfortunately, most of the maritime stakeholders use non-standardised, non-harmonised security management practices concentrating on physical threats and weaknesses, ignoring the cyber ones. Both physical and cybersecurity incidents may jeopardise the operation of the ports, vessels and the whole supply chain causing economic disruption, disruption to transport systems and to international trade. Furthermore, disrupting supply chains may

[3] (Acharya, 2019)

become a target for international terrorists if the ports and all entities within the chain have not undertaken appropriate security controls.

This report serves as an awareness raising handbook and a Best Practice Guide explaining the main issues in the security (safety and cybersecurity) of the maritime Critical Information Infrastructure (CII), the cyber threats and attacks that the maritime ecosystem (ports, ships, maritime companies, maritime supply chains) is facing due to rapid digitalisation. The consequences and impacts of these threats to the maritime operator, stakeholders, economies, and national safety can be immense. Cybersecurity standards, strategies, legal and policy instruments are presented to serve as examples of efforts to holistically address the maritime cybersecurity challenges. Risk management methodologies, tools and guidelines based on the standards are presented to raise awareness of the African ports of existing international approaches. Compliance with the standards and existing security strategies enhances resilience and collaboration which can secure international operations, supply chains and trade. Finally, recommendations are provided for the African ports and questionnaires to capture the cybersecurity maturity of the ports.

3 The European Union (EU) and African ports

3.1 Introduction

Key definitions:
Port facility: a location where the ship/port interface takes place; this includes areas such as anchorages, awaiting berths and approaches from seaward, depending on the facility [Regulation (EC) No 725/2004].

Port: a specified area of land and water, with boundaries defined by the state in which the port is situated, containing works and equipment designed to facilitate commercial maritime transport operations [Directive 2005/65/EC].

Port CIs include the port facilities (physical assets of the ports), the cyber assets and the users. According to Alderton (1999) there are 3 classical types of port ownership and operation as follows: Landlord port, Tool port and Service port.

Port Authority Responsibilities (Source: Alderton, 1999)[4]			
Port type	Infrastructure	Superstructure	Stevedoring
Landlord port	Yes	No	No
Tool port	Yes	Yes	No
Service port	Yes	Yes	Yes

The *Landlord port* is where the state, port authority or municipal council own the land and lease the terminal to private stevedores. The state provides the infrastructure such as quays and land for the terminal while the private operator provides superstructure and equipment like cranes, warehouse, terminal equipment, and other commercial facilities. An example is the Rotterdam Port Authority, which lease the port infrastructure to European Combined Terminal (ECT).

The *Tool port* is the situation where the state owns both the infrastructure and superstructure, and the private stevedore company provides the labour for operation. Competition is very high, and tenders are put into secure rights. Examples are Houston in the United States of America (USA) and most of the autonomous ports in France.

The *Service port* is also known as comprehensive or public port. The state or port authority owns both the infrastructure and superstructure and provides all services and facilities for ships. Examples include Singapore Port Authority, which was made private in 1997, and ports in India, Israel, South Africa, and Ghana.

Ports' physical layer includes docks, piers, access channels, and more. In general, the conditions from terminal to terminal within a port vary. However, all ports are challenged to maintain their infrastructure in harsh marine environments.

[4] (Alderton, 1999)

Port superstructure: the surface arrangements (such as for storage), fixed equipment (such as warehouses and terminal buildings) as well as mobile equipment (such as cranes) located in a port for the provision of transport-related port services.

Port Stevedoring: Includes loading and unloading and stowage of cargo in any form on board the vessels in Ports.

Every entity that has Port Authority responsibilities needs to identify its critical assets in the domain of its responsibility and accordingly to assess the level of risk.

Almost every asset is linked with the cyberspace in three ways, namely: 1) the technology site and the communication information systems (hardware/software); 2) the operating procedures of the technology and the communication information systems; and 3) the people and smart objects (e.g. IoT) that interact with the technology and communication information systems.

3.1.1 African Ports

African exports of goods and services have seen their fastest growth in the past decade, but the African volumes remain low at just three percent of world trade, according to the World Bank[5]. Africa's limited role in the global trade is reflected in the contours of its maritime ports, facing evolutionary challenges regarding safety, security, and cybersecurity. Nonetheless, seaports are a vital part of the supply chain in Africa with maritime transport being the main gateway to the global marketplace and with each port having a far-reaching hinterland often spanning several landlocked countries, which make up one-third of Africa. Investment and modernisation in ports and their related transport infrastructure to advance national economy and promote overall African economic development and growth is therefore vital.

A study from PricewaterhouseCoopers (PWC)[6] shows that the economic volumes handled in the major ports across Sub-Saharan Africa are mainly ports based in Western Africa and the Gulf of Guinea (see picture below).

[5] (Greater and More Diverse Participation in Global Trade is Key to Achieving Africa's Economic Transformation, says New World Bank Book, 2022)

[6] (Strenghtening Africa's gateways to trade, 2018)

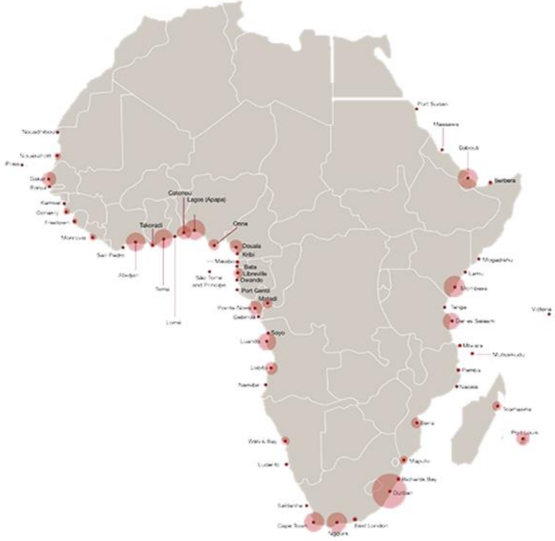


Figure 2: African Ports[7]

The countries in the Gulf of Guinea depend on protected and secure seas for their economic development, free trade, maritime transport, and preservation of the marine environment. It is a large maritime region covering 18 countries with 500 million people and stretching from Senegal to Angola with more than 5,700 km of coastline. The region is an important international shipping route, and it represents 25 percent of African maritime traffic. Oil and fish, amongst many other types of natural resources, are important commodities transported to other African countries and also to Europe and other countries worldwide by commercial vessels.

Seaports are the interface between the open sea and the hinterland. They form strategically important maritime infrastructures through which all economic goods must pass. This makes them highly vulnerable to targeting by criminal organisations and/or terrorist groups. Terrorist attacks on ports could severely impact local populations, port infrastructures themselves, and local and regional economies dependent on these port activities.

The EU remains Africa's major trading partner although its share of trade has declined while trade with China has increased. Within the African continent, West Africa is the EU's largest trading partner in Sub-Saharan Africa. Europe imports from West Africa finished products (fish and textiles), but also raw products like fuel and agricultural food products. West Africa on the other hand imports refined fuels, food products, machinery, chemicals, and pharmaceutical products from the EU. West Africa is also the most important investment destination for the EU in Africa according to UNCTAD.[8]

It is up to each individual country to decide to what extent its national security laws and the International Maritime Organization's (IMO) International Ship and Port Facility Security code (ISPS) are implemented and properly managed. There exists the opportunity to accompany

[7] (*Strengthening Africa's Gateway to Trade*, 2018)
[8] (Maritime trade and Africa, 2018)

the ports in a broad perspective to increase their security resilience. This study will act as a handbook with recommendations for port security improvements within Sub-Saharan Africa.

3.1.2 EU-African maritime business

The criticality of the maritime sector for European Member States and their economies is clearly illustrated by the fact that there are 329 European commercial ports from which 74 percent of goods imported and exported and 37 percent of exchanges within the Union transit through.

The EU and the USA are the largest trading partners with the Africa region.[9] The Global Gateway Africa – Europe Investment Package[10] aims to support Africa in:

- Accelerating the green transition
- Accelerating the digital transition
- Accelerating sustainable growth and decent job creation
- Strengthening health systems
- Improving education and training

The African Maritime Technology Cooperation Centre (MTCC) was launched in Mombasa in 2017. It is part of the Global MTCC Network (GMN) financed by the European Union[11]. The MTCC for Africa (MTCC Africa) is hosted by the Jomo Kenyatta University of Agriculture and Technology (JKUAT), Mombasa CBD Campus, in partnership with Kenya Maritime Authority (KMA) and Kenya Ports Authority (KPA).

MTCC Africa is focused on the following:

- Facilitating compliance with The International Convention for the Prevention of Pollution from Ships (MARPOL Annex VI);
- Improving capability in the region by working with maritime administrations, port authorities, government departments and shipping stakeholders to facilitate compliance with international regulations on energy efficiency for ships;
- Promoting the uptake of low-carbon technologies and operations in the maritime sector through pilot projects;
- Raising awareness about policies, strategies and measures for the reduction of greenhouse gases and other emissions from the maritime transport sector;
- Demonstrating a pilot-scale system for collecting data and reporting on ships' fuel consumption to improve ship owners' and maritime administrations' understanding in this regard;
- Disseminating and sharing results and experiences from the project through appropriate communication and visibility actions; and
- Developing and implementing strategies to sustain the impact of MTCC results and activities beyond the project time-line.

[9] (Coulibaly, Kassa, & Zeufack, 2022)

[10] (EU-Africa: Global Gateway Investment Package, n.d.)

[11] (Africa Maritime Technology Cooperation Centre launched in Mombasa, 2017); (MTCC Africa, n.d.)

Eurostatistics stated in 2021 that the largest trade partner for Africa is Europe, exporting 33 percent of its goods to Europe and importing 31 percent of their goods from there. This equates to imports of 142 billion Euro and exports, 146 billion Euro worth of goods from/to Africa in 2021.

Africa relies heavily on ships and ports to service its intercontinental trade, while the one-third landlocked countries receive their goods via countries with sea access. This means that maritime transport remains the main gateway to Europe.

Africa's maritime trade is defined by the continent's international trade concentration in the maritime ports. UNCTAD mentions that Africa’s ports account only for four percent of global containerised trade volume, much of which comprises imports of manufactured goods. Africa’s ports do not match global trends of containerisation ratios and could improve its containerised port traffic volumes and increase containerised export goods. If more cargo were transported by road from the hinterland to ports, more container vessels would enter the ports, attracting larger international traffic.

To make this happen, Africa’s ports and hinterland transport networks need to upgrade their port infrastructure and services, improve performance, enhance productivity levels, but also increase their safety, ISPS port security and cybersecurity initiatives.

4 Maritime Security Concepts

4.1 Introduction

In our security-conscious world, it is hard to recall a time when security was not a priority. Today, actions in maritime security are improving every year in various areas of the world, with a gradual decrease in accidents, injuries, physical and cyber-attacks as a result. But this kind of protection has not always been a priority for shipowners and seaports. The shift from repair to prevention has been driven by past accidents and cyberattacks on board of vessels, in seaports and maritime companies. The golden thread among these incidents was that existing security (safety and cybersecurity) rules were not followed closely and were not properly implemented in practice.

4.2 Security Concepts and Terminology

The international literature interchangeably uses the terms security, safety, cybersecurity, physical security, and resilience.

In this report, as mentioned above, the maritime CIs are considered as physical-cyber systems with physical and cyber layers. The maritime stakeholders need to ensure the security of the physical assets (safety) and the security of the cyber assets within the layers (cybersecurity). The goal of maritime safety is to protect the physical assets (e.g., ships, buildings, marinas, data centres, cargo) and people (e.g., personnel, operators, crew) against various types of physical threats e.g., intentional and unintentional incidents, dangers and harms such as physical disasters, storm at sea, fire, terrorism, social unrests, smuggling weapons and drugs, piracy. The goal of maritime cybersecurity is to ensure the confidentiality, integrity and availability of all cyber assets (e.g., telecoms, ICT, data, services) against cyber threats (e.g., phishing, spoofing, social engineering (malicious activities using human interactions), masquerading identities, non-authorised access, distributed Denial of Service (DDoS) attacks).

Security includes both safety and cybersecurity as illustrated in figure 3.

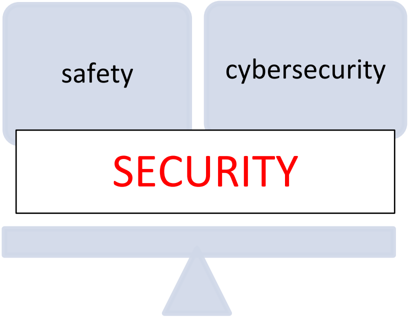


Figure 3 : Security includes safety and cybersecurity

The physical and cyber assets can be exposed to threats if appropriate controls/measures and mitigation actions have not been implemented, leaving assets vulnerable to threats and exploitation. In case an unfortunate security incident occurs, emergency security procedures, disaster recovery and business continuity plans are activated and measures undertaken taken to mitigate the risks. Whenever an incident occurs, a range of measures at the national level are triggered, in line with the emergency plans on board the ship (Ship Security Plans), in the seaport (Port Security Plan) and in the port facilities (Port Facility Security Plans).

The golden thread between safety and cybersecurity is the protection shield that is applicable in each domain. Building this protection level is done through efficient governance, trying to eliminate physical and cyber risks, avoid port security incidents and prevent human accidents. One has an impact on the other, for example, if a cybersecurity attack in a general cargo port facility suddenly stops the crane handling operation, this could cause the cargo to drop in the ship's hold and could cause a fatal injury to dockworkers below. Therefore, this study addresses **security as the composition of safety and cybersecurity** and presents how regulations, standards and best practices can be combined to address both components of security.

4.3 Maritime physical and cyber technologies

Port and vessels host complex CIIs with physical and cyber assets used to conduct their operations and provide their maritime services.

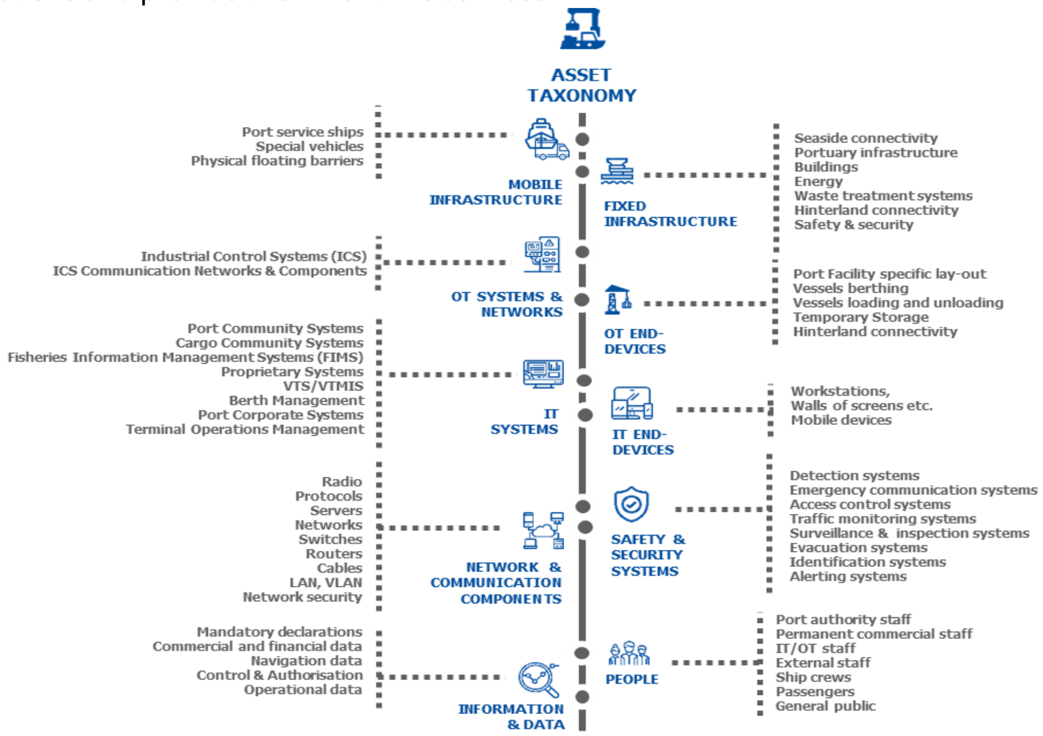


Figure 4: ENISA maritime ports' asset taxonomy[12]

Ships are armed with various technologies , including: Positioning systems, Electronic Chart Display and Information System (ECDIS), Engine Control and monitoring systems, Global Maritime Distress and Safety System (GMDSS), Automatic Identification System (AIS), Maritime ICS SCADA. The following figure illustrates the technologies onboard:

[12] (Drougkas, Sarri, Kyranoudi, & Zisi, 2019)

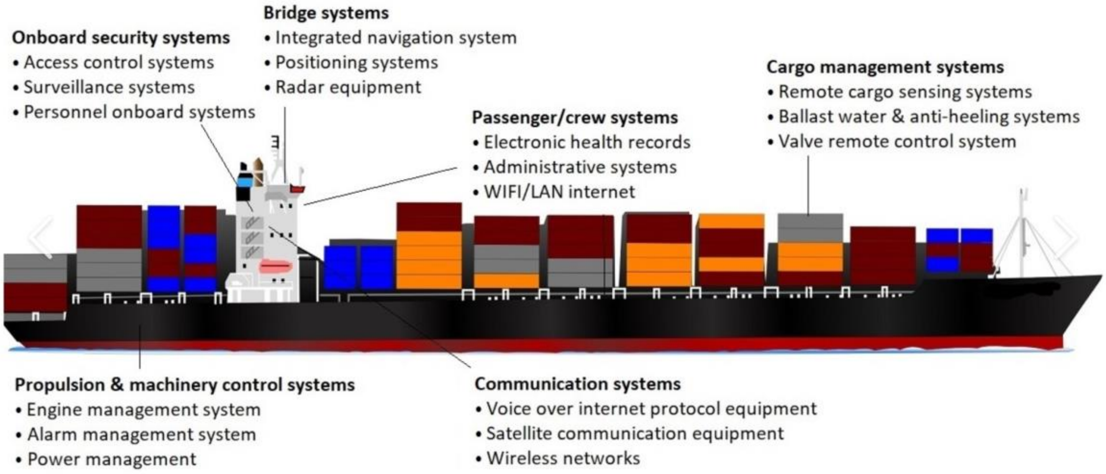
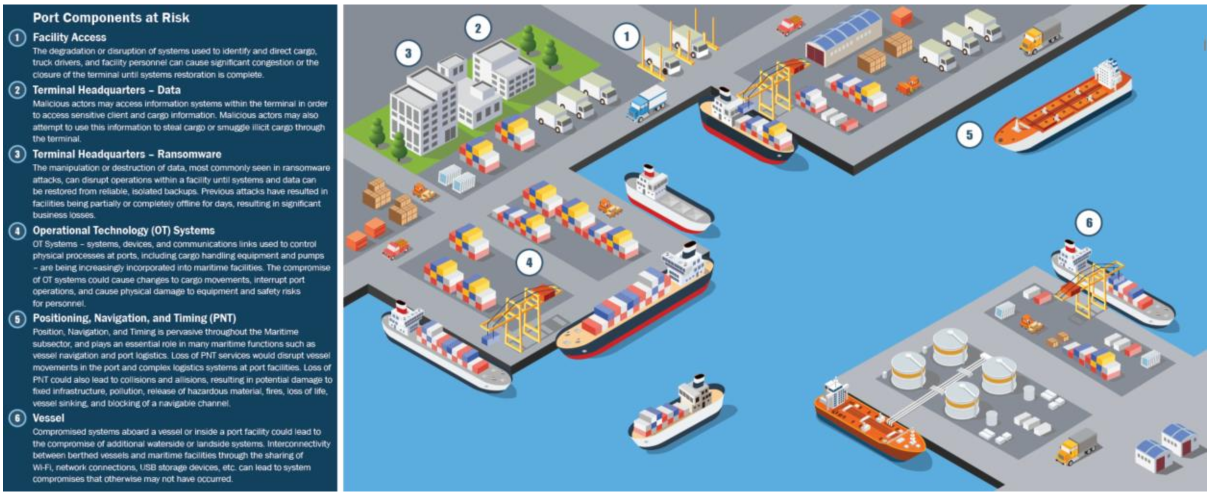

Bridge systems
• Integrated navigation system
• Positioning systems
• Radar equipment
Onboard security systems
• Access control systems
• Surveillance systems
• Personnel onboard systems
Cargo management systems
• Remote cargo sensing systems
• Ballast water & anti-heeling systems
• Valve remote control system
Passenger/crew systems
• Electronic health records
• Administrative systems
• WIFI/LAN internet
Propulsion & machinery control systems
• Engine management system
• Alarm management system
• Power management
Communication systems
• Voice over internet protocol equipment
• Satellite communication equipment
• Wireless networks

Figure 5 : Ship technologies[13]

The port and ship technologies are used to provide port and maritime supply chain services, e.g.,:

- Vessel berthing services
- Vessel loading and unloading services
- Temporary storage and staying services
- Distribution and transfer services
- Support services
- Authorities services
- Security services
- Transport of goods (e.g., Liquified Natural Gas (LNG), vehicles, grain)
- Cruise Services and transport of people
- Container Management Services
- Coastal Shipping services

[13] Source: https://www.hvassallo.com/practice-areas/maritime-cyber-security/; accessed 17 December 2022



Port Components at Risk

1. Facility Access
The degradation or disruption of systems used to identify and direct cargo, truck drivers, and facility personnel can cause significant congestion or the closure of the terminal until systems restoration is complete.

2. Terminal Headquarters – Data
Malicious actors may access information systems within the terminal in order to access sensitive client and cargo information. Malicious actors may also attempt to use this information to steal cargo or smuggle illicit cargo through the terminal.

3. Terminal Headquarters – Ransomware
The manipulation or destruction of data, most commonly seen in ransomware attacks, can disrupt operations within a facility until systems and data can be restored from reliable, isolated backups. Previous attacks have resulted in facilities being partially or completely offline for days, resulting in significant business losses.

4. Operational Technology (OT) Systems
OT Systems – systems, devices, and communications links used to control physical processes at ports, including cargo handling equipment and pumps – are being increasingly incorporated into maritime facilities. The compromise of OT systems could cause changes to cargo movements, interrupt port operations, and cause physical damage to equipment and safety risks for personnel.

5. Positioning, Navigation, and Timing (PNT)
Position, Navigation, and Timing is pervasive throughout the Maritime subsector, and plays an essential role in many maritime functions such as vessel navigation and port logistics. Loss of PNT services would disrupt vessel movements in the port and complex logistics systems at port facilities. Loss of PNT could also lead to collisions and allisions, resulting in potential damage to fixed infrastructure, pollution, release of hazardous material, fires, loss of life, vessel sinking, and blocking of a navigable channel.

6. Vessel
Compromised systems aboard a vessel or inside a port facility could lead to the compromise of additional waterside or landside systems. Interconnectivity between berthed vessels and maritime facilities through the sharing of Wi-Fi, network connections, USB storage devices, etc. can lead to system compromises that otherwise may not have occurred.

Figure 6: Port Technologies[14]

4.3.1 Accelerated Maritime Digitisation

The adoption of emerging technologies including Artificial Intelligence (AI), 5G, Big Data, IoT, robotics and satellite technologies is being used for new maritime advancements, e.g., autonomous vessels, rapid inspection of ports CIs including wind energy facilities, underwater benthic stations, automation of geophysical and geotechnical seismic surveying operations, monitoring and managing ships.

The accelerated adoption of the digital technologies in the maritime ecosystem will lead to numerous innovations in various maritime functions e.g., exchange massive amounts of information using advanced acoustic and optical communication networks, automate decisions collectively, sharing of complementary resources, automate port and ships maintenance and operations. However, these forthcoming innovations will be accompanied with new physical and cyber threats. Security (safety and cybersecurity) governance will be necessary to ensure that port authorities, shipowners and all maritime stakeholders possess the tools, knowledge, and structure in place to maximise the security performance of their infrastructures (ports, on board of their ships) and obtain their security objectives, in accordance with the maritime security legislation and international best practices.

4.4 Security Incidents and Threat Actors

Each port, needs to develop bespoke working governance with efficient (physical and cyber) risk management practices that ensure the security of the maritime CIs, operations and services.

4.4.1 Types of Attackers

Cybercriminals are adversaries that perform an illegal action using digital means. For example, if the impact of the attack is illegal (e.g., theft, crime, vandalism, terrorism) then he/she is characterised as a cybercriminal. Adversaries are classified further according to their motivations, opportunities, and capabilities:

[14] Source: (Burt, 2021)

- *Intentional Actors*: insider attackers are a class of threats with detailed knowledge of an organisation and its systems.
- *Cyber Terrorists:* perform violent activities to influence public opinion and decision making.
- *Hacktivists / Civil Activists*: for ideology reasons conducts attacks to draw attention to a political, social, religious, or moral agenda.
- *(Organised) Cyber Criminal:* their goal is to obtain a financial profit, influence elections, abuse people. All traditional criminal activities that are conducted using digital means belong in this category.
- *Script Kiddies:* non-mature agents with little knowledge and capabilities, with usual motive to have fun, to win a bet or a prize.
- *State-Sponsored Attackers / Government Spies* operate to obtain access to privileged information, such as intellectual property, business plans, roadmaps, personnel or customer data, etc. and insight into business operations and upcoming decision making.
- *Competitors / Commercial Industrial Espionage Agents* try to gain a commercial advantage through the theft of intellectual property, documentation on business operations and decisions or customer data.
- *Government Cyberwarriors / Individual Cyber Fighters* are patriotically motivated types of actors. They are either directly controlled by a nation or are individuals or groups of people driven by their political, social, ethnical or religious values.
- *Cyber Vandals' / Cyber Punks'* main motivation is the destruction of property, driven by the quest of personal satisfaction and dominance.
- *Blackhat Hackers / Crackers* try to gain access to systems out of curiosity and personal gain, which may range from financial rewards from exploiting obtained data, products and systems, or in terms of reputation and recognition among their peers.

There are also *Unintentional Actors*, who are usually untrained or reckless employees who still have the potential to cause harm to the organisation. They do not have malicious intent but are mentioned as their actions can still represent a security risk.

4.4.2 Security Incidents

Port and ship operations are increasingly dependent on the effectiveness of software-based systems for operations, and those ships and ports that can take advantage of new technologies and digital solutions will be better off than others. For example, communication between ships and port cargo handling operations requires information transfer via computers. These information technology (IT) systems handle all administrative tasks for the preparation, execution, and handling of cargo. Terminal handling machines, such as container cranes, and machinery on board ships have digital connections to other remote-control systems. These mechanical machines with digital equipment are called Operational Technology (OT) systems. It can generally be said that OT systems control the physical world, such as machines, while IT systems manage data/information. The latter manages the flow of digital information (data), while the former manages the operation of physical processes and the machinery used to carry them out. In the maritime world, OT refers to ship and port hardware, systems and software that operate ships and port handling equipment and monitor and control physical devices and processes, and IT refers to the computers and servers in the offices used to manage information processing, including software, hardware, and communication technologies.

These OT and IT systems are not always well protected against a cyberattack. The risks with IT systems mainly affect finances and reputation, while OT systems can affect and threaten port infrastructure and even cost lives. Seaports and ships may seem like unusual targets for cyberattacks, but these attacks increasingly target maritime operators and successful attacks are regularly reported worldwide. Therefore, cybersecurity is becoming increasingly important to resist cyberattacks in the maritime sector.

For a long time, senior management at ports and shipping companies have viewed cybersecurity and risk management as a task for the IT department, but this is rapidly changing as all personnel is involved in managing and helping mitigate cyber risks.

The impact of a cyberattack can propagate in physical assets e.g., a cyberattack can disable the smart fire detection system and automatic extinguishing systems on an LNG tanker at a major port in Africa and start a fire. Cyberattacks and any type of security/safety incident can negatively impact the maritime supply chains and local and international trade. For example, a cyberattack on the electronic navigation system can disorient a ship, making it collide and sink at the entrance to a major EU or African port. It could take weeks to remove the wreckage and return the port to service with economic, legal, and business damages to the African and European supply chains caused by the disruption of trade.

Ships could be used as a means of transportation for terrorists or to smuggle weapons into a country but could also be used to detonate a bomb on the ship to blow up a critical part of the port. However, a 2018 cybersecurity survey[15] found that few shipping companies are ready to weather a cyberattack without much damage. The need for guidelines and relevant laws are more than clear in the industry. Ports need to implement an effective governance plan covering physical and cybersecurity governance procedures and processes.

4.4.2.1 Safety Accidents

Several maritime accidents and fatal ship disasters are considered security incidents. For example, the sinking of the RMS Titanic in April 1912 was one of the first passenger vessels that sank with a loss of more than 1,500 lives. This disaster and the large number of casualties was due to reckless sailing near icebergs and insufficient lifeboats to save everyone on board.[16] Another example is the sinking of the Ferry M/S Estonia in 1994, where the cargo deck bow was not closed watertight and opened in a storm, resulting in sinking and the loss of more than 850 passengers.[17] A similar accident occurred with the Ferry Herald of Free Enterprise in 1987, leading to the loss of 197 people and the entire ship with its cargo.[18] The fatal tanker explosion of the Motorvessel M/V Bow Mariner in 2004, loaded with ethanol,

[15] (Jørgensen, 2018)

[16] (Titanic, n.d.)

[17] (Langewiesche, 2004)

[18] (Herald of Free Enterprise Ferry Disaster – 1987, n.d.)

exploded, sank and put 21 crewmembers in a sea grave. The reason for this disaster[19] was the violation of several safety regulations that caused the explosion and then increased the death toll. A more recent accident, the Costa Concordia disaster in 2012 was caused when the captain sailed too close to the rocks, resulting in the loss of the vessel and 32 lives.[20]

In seaports, many accidents can happen in relation to ships' unloading and loading operations, but also in terminals and in the common port area. A study carried out by R. Darbra and J. Casal[21] on hundreds of accidents that occurred in seaports concluded that the most frequent accidents were gas releases (51 percent), followed by fires (29 percent) and explosions (17 percent). More than half of the accidents occurred during loading and unloading operations, but storage warehouse accidents, chemical plant accidents and operations within the port area also contributed significantly to the total number. One of the most recent examples of a serious accident was in the port of Beirut in August 2020, where a huge blast devastated parts of Beirut was blamed on the detonation of 2750 tons of ammonium nitrate that had been stored in the port of Beirut after the seizure of a vessel.[22]

4.4.2.2 Cyberattacks

Cyberattacks on maritime infrastructure can be varied. Listed hereunder some examples of recent cyberattacks in order to raise the readers' attention to the potential threats of such malicious acts and to further analyse the mechanisms of these attacks.

- On April 10, 2020, a malware attack targeted the Mediterranean Shipping Company (MSC).[23] For security reasons, MSC's servers were shut down to protect company data and MSC's website was taken offline. The attack disrupted internal data processes.
- On July 8, 2019, a malware attack targeted a ship bound for New York Harbour, resulting in the loss of critical data. The Coast Guard reported that a lack of security strategies on the ship was the main reason for such an attack.[24] All crew members on the ship shared the same login and password for the ship's computer. In addition, the hacker took advantage of the use of external devices and a lack of antivirus software.
- In March 2019, a ransomware attack completely crippled the global network of shipping company Norsk Hydro when they fell victim to the LockerGoga ransomware. Norsk Hydro estimated that the hackers had been in their network for two to three weeks before they were discovered. More than 22,000 computers and thousands of servers in five countries were affected, and LockerGoga shut down production and office operations for days. Damage was estimated at 71 million dollars.[25]
- In 2018, the Chinese government is suspected of having carried out a ransomware attack on a U.S. Navy contractor and stealing highly sensitive security data, including plans for a supersonic missile project.[26]

[19] (Shapira, 2006)
[20] (Costa Concordia: What happened, 2015)
[21] (Darbra & Casal, 2004)
[22] (The Beirut Port Explosion, n.d.)
[23] (Hand, 2020)
[24] (Winder, 2019)
[25] (Tomter & Gundersen, 2019)
[26] (China hackers steal data from US Navy contractor - reports, 2018)

- In September 2018, cyberattacks hit the ports of Barcelona (Spain) and San Diego (USA). The ransomware attack on the port of San Diego turned out to be an infection of the SamSam malware.[27] The impact was limited to some administrative functions of the port authority and did not interrupt port operations or ship movements. The Port of Barcelona did not immediately disclose the type of incident but indicated that the attack had disrupted its internal IT systems although it did not affect ship or port operations.
- In July 2018, China Ocean Shipping Company (COSCO) also fell victim to the SamSam ransomware. When SamSam struck, it disrupted COSCO's networks in the United States, Canada, Panama, Argentina, Brazil, Peru, Chile, and Uruguay. It took 5 days for the company to get back online.
- A.P. Moller-Maersk Group was hit by a devastating attack in June 2017 due to the NotPetya malware.[28] Maersk had to cease operations for 10 days to recover from the attack, which involved reinstalling 4000 servers, 45,000 PCs and 2500 applications. Maersk reportedly lost approximately 300 million dollars in revenue.

The table below lists the top cyber threats for 2022 according to the European Union Agency for Cyber Security (ENISA) with the Cyber Risk Management of the Ports.

Cyber threat	Cyber Incident			Reference
	Affected Organisation	Date	Impact	
Malware/ Ransomware	IT systems	2022	Major Oil Terminal Europe	https://www.france24.com/en/live-news/20220203-european-oil-port-terminals-hit-by-cyberattack
Malware/ Ransomware	Oil Companies	2022	Port of Antwerp	https://www.dw.com/en/belgium-investigates-cyberattack-on-energy-companies/a-60651892
Malware	IT systems	2021	Oil tanking Deutschland GmbH & Co. KG	https://www.bbc.com/news/technology-60215252
Malware/ Ransomware (Mailto)	Toll Group	2020	Data destruction	https://www.itnews.com.au/news/toll-group-hit-by-new-variant-of-mailto-ransomware-537537
Malware	Mediterranean Shipping Company (MSC)	2020	Network outage	https://www.wsj.com/articles/mediterranean-shipping-co-hit-by-network-outage-considering-potential-cyberattack-11586523861
Malware	CMA CGM	2020	Security Breach	https://www.reuters.com/article/uk-cma-cgm-cyber-idUKKBN26L2N0
Malware/ Ransomware	Administrative Services of the Port	2018	Port of San Diego and Barcelona	https://www.acronis.com/en-us/blog/posts/ransomware-attacks-sail-san-diego-and-barcelona/

[27] (Port of San Diego: phishing emails remain amongst greatest cyber threats, 2021)
[28] (Greenberg, 2018)

Malware/ Ransomware	COSCO	2018	Local network breakdown	https://www.forbes.com/sites/leemathews/2018/07/26/another-shipping-giant-falls-victim-to-ransomware/?sh=6aa75bd70d04
Malware/ Ransomware (NotPetya)	A.P. Moller–Maersk	2018	Data destruction	https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html
Breach of Data	Service of the Port controlled the movement and location of containers	2013	Port of Antwerp	https://www.bbc.com/news/world-europe-24539417

Geopolitical changes also impact the security of the maritime operations. During the Ukraine war in 2022, the vessels navigating in the Black Sea and the Sea of Azov experienced a series of cyber-attacks. The US Maritime Administration (MARAD) reported that the vessels became cyber victims of GPS interference, AIS spoofing and communications jamming. The NATO Shipping Centre and US Maritime Administration reported DDoS attacks on these vessels.

4.4.2.3 IT/OT attacks

Many ships still use IT and OT information systems and technologies that are not built to withstand cyberattacks. If they are not properly protected, hackers can exploit the vulnerabilities. If they can control the ship's system remotely, they could take over the command-and-control communication information systems. A ship is an integrated system-of-systems. This is the reason why the critical information infrastructures systems of the ship need to be defined and assessed, and security monitored on a continual base and inspected regularly. Other activities hackers could do include:

- spoof the navigation systems
- control the ships autopilot
- jam or clutter the ships radars
- control the engines and vessel speed
- destabilise the ships by transferring/flooding ballast water
- seriously damage equipment, e.g., by taking a vital cooling system offline
- shut down vital cargo systems like reefer power supply
- shut down fire detection and extinguishment systems
- take control of the rudder long enough to direct the ship into the dock at full speed

Therefore, ships must use technological solutions and operational principles to avoid these types of situations. The solutions are described in this study in chapters 5 and 6.

The same applies to ports where IT and OT systems are also in constant use. Within the security domain of ports and ISPS-compliant terminals, it is important to consider the following:

- the Security Management System (SeMS) is efficient only if it is digitised.
- the ID badge system is efficient when it is a digital system based on a common database to which law enforcement and customs also have access.
- the automatic barrier system admits only persons entitled to enter the zone.

- a perimeter monitoring system with a high-performing closed-circuit television (CCTV) or other camera system will take smart actions and can track video footage for long periods of time.

More details on this are included below.

4.4.2.4 The use of computers to communicate between stakeholders enables real-time and efficient action when needed. Supply Chain and hybrid threats

Maritime supply chains are the blood veins of global trade and economy, and involve cross border collaboration to offer critical complex services (e.g., container management, vehicle transport, LNG storage and transport, cruising). Most physical processes within a maritime service (e.g., vehicles and cargo loading/unloading, LNG distribution and storage) are executed with autonomous or semi-autonomous mechanical physical systems and machineries (e.g., ships, trucks, cranes, electronic gates/fences) under the control of sophisticated logistic software systems (e.g., Industrial Cyber-Physical Systems, SCADA, surveillance systems). In addition, cargo ships are connected with the ports and the other operators via a plethora of communication and data links (e.g., satellite communications or conventional radio communications) and their navigation is today widely reliant on electronic solutions (e.g., satellite navigation with GPS, Galileo or Electronic Chart Display Information Systems, (ECDIS)). Thus, maritime supply chains can be viewed as complex physical-cyber systems composed by heterogeneous, interconnected physical and cyber assets, owned by different national, EU and international CIs ensuring seamless and swift product/data exchange from the producer down to the end consumer during the provision of these services.

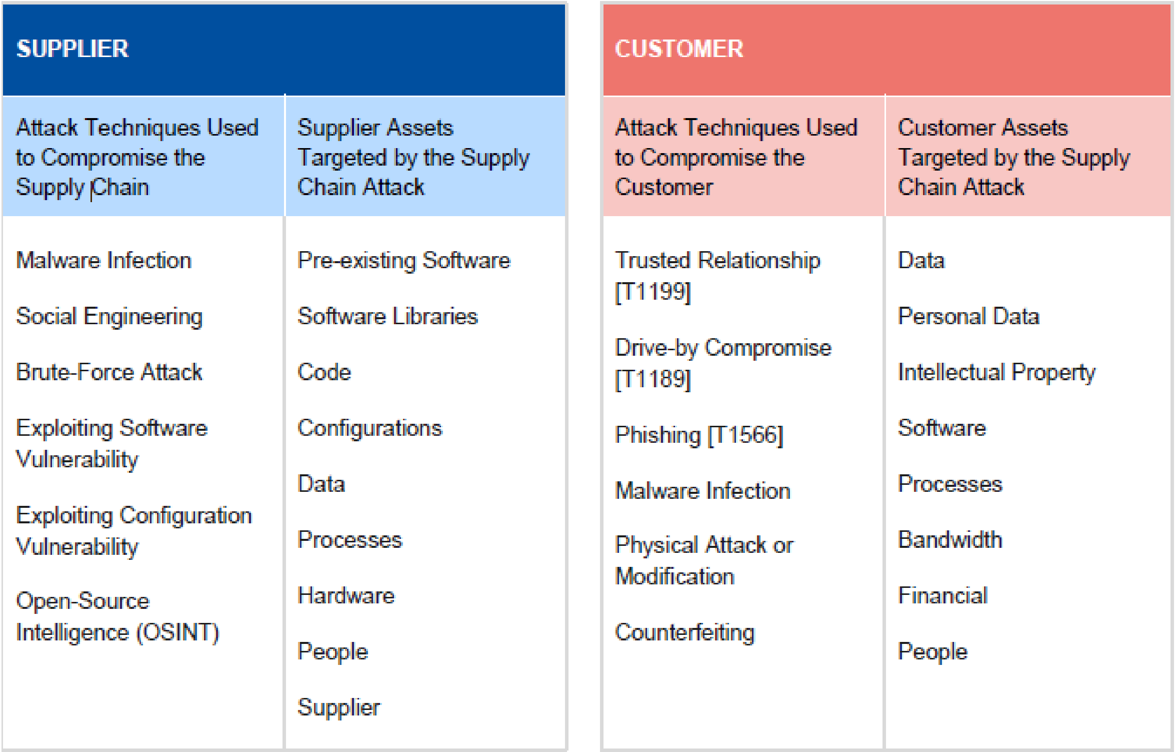
The interconnection of physical and cyber assets exposes the maritime ecosystem to **hybrid threats** where attacks on physical assets propagate to the cyber assets and vice-versa.

Attacks on maritime supply chain services cause not only disruption of the services, but tremendous damage to maritime operations, international safety, economies, societies, and the environment. For example, attacks in the Industrial Control Systems (ICS) (e.g., supervisory control, SCADA, distributed control systems and programmable logic controllers) hosted in ports or maritime transport companies may cause disruption or damage to critical mechanical devices (e.g., container cranes, safety and mechanical systems that operate locks and dams) and worse they may cause loss of life, stealing of cargo, destruction of a ship. The effects (in terms of thermal radiation, overpressure blast wave and flying shrapnel) of the explosion of an LNG tanker or in the ports' LNG storage facilities or terminals due to a hacked SCADA system, could lead to a loss of energy stock, which could be critical during the winter. It could also impact negatively on the environment (degradation, fragmentation or loss of ecosystems), the economy and more importantly the wellness and health of citizens. An attack on a container terminal management system could disrupt intermodal container services involving maritime, rail and truck transportation.

Cyberattacks (e.g., inserting a malware) in the ports' SCADA systems may cause fuel spills affecting water quality; attacks in the PCS may turn LNG tankers into floating bombs; physical attacks (e.g., bombing) in a dry bulk storage area of coal products may create and carry dust by wind to tourist terminals or nearby residences. Modern surveillance systems, monitoring units, sensors, RFIDs, marine traffic systems, PCS, Automated Border Control Systems are susceptible to current threats. They are prone to snooping, interruption, vandalism, and interception which may cause the disruption of various critical maritime operations and services as well as their use in human and drug trafficking and terrorism. It should be noted that according to 2016 estimates by the RAND Corporation and the USA Congressional Research Service, an attack on a ports' CI could cause tens of thousands of deaths and cripple global trade, with losses ranging from 45 billion dollars to more than 1 trillion dollars.

The International Port Community Systems Association in 2015 recommended that all maritime, logistics, supply chain actors and PCS operators – with the support of their trade associations and international and regional bodies – address the current threats to the supply chain. Additionally, it recommended to bring together key stakeholders in the supply chain to create an Information Sharing and Analysis Centre (ISAC) to discuss cybersecurity threats, risks and experiences.

ENISA has published the most important supply chain threats, shown below.[29]



SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Malware Infection Social Engineering Brute-Force Attack Exploiting Software Vulnerability Exploiting Configuration Vulnerability Open-Source Intelligence (OSINT)	Pre-existing Software Software Libraries Code Configurations Data Processes Hardware People Supplier	Trusted Relationship [T1199] Drive-by Compromise [T1189] Phishing [T1566] Malware Infection Physical Attack or Modification Counterfeiting	Data Personal Data Intellectual Property Software Processes Bandwidth Financial People

Figure 7: Proposed taxonomy by ENISA for supply chain attacks.

It has four parts: (i) attack techniques used on the supplier, (ii) assets attacked of the supplier, (iii) attack techniques used on the customer, (iii) assets attacked of the customer.

[29] (Threat Landscape for Supply Chain Attacks, 2021)

4.4.2.5 Threat Vectors

Based on multiple resources [30, 31, 32, 33, 34 and 35] the usual maritime cybersecurity threats and the maritime assets targeted using specific techniques are listed below:

Threats	Techniques	Maritime Assets and Services as Targets
Ransomware	Initial Access	People, IT Systems, IT end-devices, Network & Communication Components, Information and data etc.
	Execution	IT Systems, IT end-devices Network & Communication Components, etc.
	Persistence	People, Authority Services, Support Services etc.
	Privilege Escalation	People, IT Systems, IT end-devices, etc.
	Defence Evasion	IT Systems, IT end-devices Network & Communication Components, Mobile Infrastructure, Fixed Infrastructure, etc.
	Credential Access	People, IT Systems, IT end-devices, etc.
	Discovery	People, IT Systems, IT end-devices, Network & Communication Components, etc.
	Lateral Movement	People, IT Systems, IT end-devices, Network & Communication Components, Information and data, etc.
	Collection	Information and data, Vessel berthing services, Security and safety services, people, support services, Temporary storage and staying services Distribution and transfer services, etc.
	Command and Control	IT Systems, IT end-devices, Network & Communication Components, Information and data, Vessel berthing services, Vessel loading and unloading services, Distribution and transfer services, Mobile Infrastructure, Fixed Infrastructure, OT Systems & Networks, etc.
	Exfiltration	IT end-devices, IT systems, Network & Communication Components, o OT Systems & Networks, etc.
	Impact	IT Systems, IT end-devices, Network & Communication Components, Information and data, etc.
Malware	Breach on security	IT end-devices, IT systems, Information and Data etc.
Social Engineering	Reconnaissance	People, IT systems, Authorities services, Security services, Security Systems, etc.
	Resource Development	People, IT systems, Authorities services, Security Systems, Information and Data etc.
	Initial Access	People, IT systems, OT Systems & Networks, IT end-devices, OT end-devices, etc.
	Execution	People, IT systems, etc.

[30] (Ashraf, et al., 2022)
[31] (ENISA Threat Landscape 2022, 2022)
[32] (Guidelines - Cyber Risk Management for Ports, 2020)
[33] (Alcaide & Garcia-Llave, 2020)
[34] (Meland, Bernsmed, Wille, Rødseth, & Nesheim, 2021)

Threats against availability (DDoS)	Resource Development	IT Systems, IT end-devices, Network & Communication Components, Information and data, Mobile Infrastructure, Fixed Infrastructure, etc.
	Defence Evasion	IT systems, IT end-devices, Network & Communication Components, etc.
	Impact	IT Systems, IT end-devices, Network & Communication Components, Information and data, Mobile Infrastructure, Fixed Infrastructure, Vessel berthing services, Vessel loading and unloading services, Distribution and transfer services, Support services, Authorities services, Security services, etc.
Threats against availability (Internet Threats)	Initial Access	IT end-devices, IT systems, Network & Communication Components, etc.
	Discovery	IT end-devices, IT systems, Network & Communication Components, etc.
	Collection	IT end-devices, IT systems, Network & Communication Components, etc.
	Impact	IT end-devices, IT systems, Network & Communication Components, etc.
Disinformation - Misinformation	Reconnaissance	People, IT end-devices, IT systems, Information and Data, etc.
	Resource Development	People, IT end-devices, IT systems, Information and Data, etc.
	Initial Access	People, IT end-devices, IT systems, etc.
	Execution	People, IT end-devices, IT systems, etc.
	Impact	People, IT end-devices, IT systems, etc.
Supply Chain Attacks	Reconnaissance	Both Supplier and Customers (Table of Threat Landscape for Supply Chain Attacks)
	Resource Development	Both Supplier and Customers (Table of Threat Landscape for Supply Chain Attacks)
	Initial Access	Both Supplier and Customers (Table of Threat Landscape for Supply Chain Attacks)

5 Maritime Security Standards and Strategies

In this chapter the standardisation organisations and policy bodies are presented, and the maritime security (safety and cybersecurity) standards and their goal are outlined.

5.1 Introduction

For over a decade, significant effort has been made in the introduction of risk management and assurance methodologies for CIIs concentrating either on the cyber or on the physical threats ignoring the complex dual nature (physical and cyber) of the maritime CIIs. In this chapter, the relevant maritime security standards are summarised and in the last section, guidance is provided on what to use for which threat.

5.1.1 European Maritime Security Strategy (EUMSS)

The First Maritime Security Strategy was adopted on 24 June and 16 December 2014 as a response to modern risks and threats to global maritime security. The Strategy promotes better civil-military cooperation and coordination between internal and external security actors such as the police and defence. The aim is that this joined-up approach to maritime security promotes closer cooperation between different maritime sectors and makes the EU's maritime security policy more coherent, effective, and cost efficient. This toolkit explains how the Action Plan is to be implemented and highlights the European External Action Service (EEAS) activities and the role for EU delegations and EEAS HQ services.

The Revised EU Maritime Security Strategy adopted in June 2018 allows for a more focussed reporting process to enhance awareness and better follow-up to the First strategy. The action plan brings together both internal and external aspects of the Union's maritime security, facilitates a strategic, cross-sectoral approach and establishes a joint civil-military agenda for maritime security research (including dual use).

The revised strategy stresses that better coordination should be ensured in implementing EU strategies and policies with cross-cutting objectives such as those in the areas of energy, environment and security threats and challenges, including cyber and hybrid threats, terrorism, and organised crime. It highlights the changing nature of threats in the maritime domain and calls for renewed commitment to the protection of critical maritime infrastructure, including underwater, and maritime transport, energy and communication infrastructure, *inter alia* by enhancing maritime awareness through improved interoperability and streamlined information exchange (mandatory and voluntary). It calls for improving the protection and resilience of maritime systems and infrastructure. In this regard, relevant EU policies and initiatives are considered.

One the main actions mentioned is the revised A.3.8: "Improve the integration of a cybersecurity dimension in the maritime domain in terms of capabilities, research and technology and industry, building on civil-military coordination and synergies with EU cyber policies related to both cybersecurity and cyber defence, in line with the NIS Directive and international recommendations and regulations such as SOLAS XI-2 and the ISPS Code and their future updates. This will include exchange of best practices and development of joint projects by EU Member States on maritime cyber-attack prevention."

Action A.4.3 states "Pursue a comprehensive approach to maritime security risk management, in particular by conducting common risk analysis and identifying possible gaps and overlaps in this domain, while also taking into account cyber and hybrid threats, climate challenges and maritime environmental disasters."

Action A.4.8 states: "Develop a network of experts on cyber-security and cyber-defence for the maritime field to develop guidelines on procedures in response to emerging threats in the maritime field including possible acts of terrorism and other intentional unlawful acts at sea, especially as regards protection of ships, cargo, crew and passengers, ports and port facilities, marine energy installations and other critical maritime and energy infrastructure, in line with both the NIS Directive and the ISPS Code." Building capabilities and enhancing the cybersecurity education and training in the maritime field in collaboration with all stakeholders (e.g., UN, the International Labour Organization (ILO) and IMO and NATO) is also among the actions of the revised strategy (Action A.5.1, A.5.6).

The EUMSS covers both the internal and external aspects of the Union's maritime security; contributes to a stable and secure global maritime domain, in accordance with the European Security Strategy. The Directorate-General (DG) MARE is the European Commission body responsible for the development of the strategy with the collaboration of various DGs (e.g., DG CNECT, DG MOVE, DG ECHO, DG RTD) and agencies (e.g., European Maritime Safety Agency (EMSA), ENISA). The EU Security Union Strategy 2020 promotes strategic autonomy and resilience for EU supply chains in terms of critical products, services, Infrastructures and technologies.

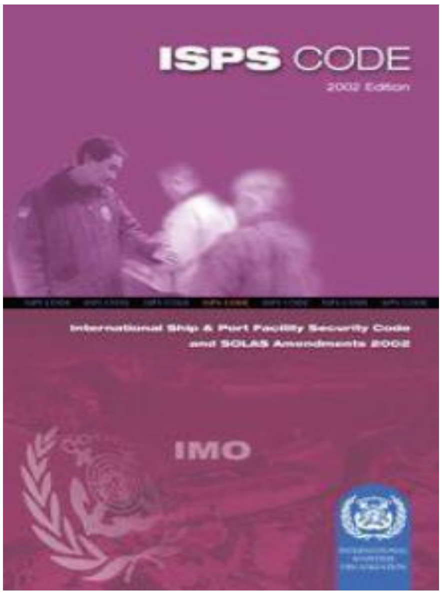
5.1.2 Maritime Safety standards

Maritime organisations (e.g., IMO, BIMCO, EMSA) have issued various safety related standards and guidelines, several of which are detailed below.

5.1.2.1 The ISPS Code

The most important is the IMO International Ship and Port Facility Security (ISPS) Code which is the international code for the security of ships and port facilities, established by the IMO, within the International Convention for the Safety of Life at Sea (SOLAS) 1974 regulation (chapter XI-2).[35]

[35] (SOLAS XI-2 and the ISPS Code, n.d.)



ISPS CODE
2002 Edition
International Ship & Port Facility Security Code
and SOLAS Amendments 2002
IMO

The ISPS Code provides a framework through which ships and port facilities can co-operate to detect and deter acts which pose a threat to maritime security. The Code provides an approach to establish security governance in the maritime CIs. It:

- enables the detection and deterrence of security threats within an international framework;
- establishes roles and responsibilities;
- enables collection and exchange of security information;
- provides a methodology for assessing security;
- ensures that adequate security measures in place.

The code consists of two parts with mandatory requirements and guidelines for ship and port facility security. Part A contains mandatory requirements and Part B contains implementation recommendations to enhance security. In this regard, the principles behind the ISPS Code are like the ISM code on board a ship. Before the ISPS Code is legally enforceable in a country, it must be transposed into a national law. Some countries adopted the ISPS Code shortly after July 2004, but other countries did not adopt it until years later. Some countries have adopted the code in its entirety, and some have made variations to the national ISPS Code regarding certain aspects of port security.

The European Union[36] immediately implemented Part A of the code at its ports and decided to also treat Part B as mandatory rather than merely a recommendation. African countries implemented the code independently via their national legislation.

It is important to highlight that the ISPS Code uses the word "port facility", meaning the port is not under the ISPS umbrella. The "port" security aspects are addressed in the Code of Practice (COP) on Security in ports.

[36] Directive 2005/65/EC on enhancing port and adjacent areas security

The 2003 Geneva COP on port security complements the provisions of the ISPS Code in terms of ensuring the security of the wider port area. The code defines security functions, duties, and measures to deter and respond to criminal acts against ports. It uses the same practices and principles as in the ISPS Code and is a guide for all port security beyond the port facilities area. The European Union introduced the code as a mandatory guideline[37] for improving its port security.

5.1.2.1.1 Construction security

From the moment a ship is built, security begins with the requirement that a vessel be seaworthy before it leaves shore, as required by Lloyds of London (P&I Club).[38] Each merchant vessel is registered by a flag state, whether it is the shipowner's country of residence or a country flying a flag of convenience. They must comply with the maritime rules, regulations and provisions of the specific flag state, in accordance with international maritime rules and provisions of the IMO and must be certified by a classification society.

However, some flags of convenience have reduced security, do not have adequate resources to carry out proper inspections, and do not impose sanctions on ships in violation. This results in ships that fail to meet several critical security requirements, but which are sometimes still allowed to dock in certain ports. Since these unsafe ships focus only on repairing parts of the ship when defects occur rather than focusing on preventive maintenance, the risk of an accident is high.

5.1.2.1.2 Port State Control (PCS)

It is the responsibility of the flag state (the country where the ship is registered) to ensure that a vessel meets all the required security standards. PSC acts as an effective backup for the inspections that are done regularly by flag states to detect substandard vessels.

PSC is thus the IMO maritime safety (physical security) initiative that aims to verify a ship's compliance with international conventions and standards. They help to lower the risk of ship hazards. The role of PSC is to highlight potential security (safety and cyber) risks and to address these to the flag state of the ship. During ship inspections, PSC verifies that the condition of the vessel and its handling equipment comply with the requirements of international IMO regulations and that the ship is manned and operated in compliance with these rules. They work according to a cooperation resolution for controls of ship and discharging (IMO Resolution 682 17).[39]

5.1.2.1.3 Vessel safety operations standards

Seafarers are the human factor that can keep risks on board low. This role is led by the onboard safety officer, who is appointed to keep the safety management plan up to date, utilise a Safety Management System (SMS) and keep the crew alert by means of safety training. The backbone of safety governance is the SMS, as its main purpose is to provide a systematic approach for managing safety risks in ship operations. SMS makes part of the

[37] Directive 2005/65/EC on enhancing port and adjacent areas security

[38] (Rulebook 2021)

[39] (Resolution A.682 (17), 1991)

International Safety Management (ISM) code[40] and commercial vessels are required by IMO to establish safe ship management procedures.

One of the most important aspects of keeping the integrity of the vessel during a sea voyage is to have the cargo well-secured. Lateral and longitudinal forces on the vessel created by swell during storms are an enormous risk to the stability of the vessel due to the risks of shifting cargo. All cargo should be stowed and secured in such a way that the ship and crew are not put at risk. Proper lashing and securing procedures are to be followed, in accordance with the IMO CSS code[41]. If a malicious attack makes the cargo unsecured and free moving in the hold, the risk of losing the ship and crew is real.

5.1.2.1.4 Curative safety aspects on board of vessels

In case an accident on board happens, it is vital that the crew is trained to immediately minimise the impact of the harm done. Therefore, crew members are trained in crisis management principles and emergency response procedures towards all types of accidents and how to fight a fire. The Seafarers' Training, Certification and Watchkeeping (STCW) code[42] and SOLAS address these aspects in detail, but this expertise domain falls out of the scope of this study.

5.1.2.2 Other important codes

- IMO's International Maritime Solid Bulk Cargoes Code (IMSBC Code);
- International Code for the Construction and Equipment of Ships carrying Dangerous Chemicals in Bulk (IBC Code);
- International Code for the Safe Carriage of Grain in Bulk (International Grain Code);
- Code of Practice for the Safe Loading and Unloading of Bulk Carriers (BLU Code);
- International Maritime Dangerous Goods (IMDG) Code;
- EMSA[43] provides tools for EU maritime stakeholders e.g., AIS, SafeSeaNet for vessel traffic monitoring, CleanSeaNet satellite images for identifying pollution at sea, EMCIP for centralising data on marine accidents, training tools, etc.
- The European Sea Ports Organisation[44] promotes the green ports and energy efficiency efforts, and is specialised in safety guidelines and training related to ship operations at ports, for example: LNG bunkering, waste reception, load and unload of general goods, containers and bulks, and container movements.
- The ILO[45] has published the ILO code of practice on safety and health in ports; the ILO code provides relevant guidance for the management, operation, maintenance, and development of ports.
- The USC Container Security Initiative (CSI)

[40] (The International Safety Management (ISM) Code)
[41] (Code of Safe Practice for Cargo Stowage and Securing (CSS Code), n.d.)
[42] (International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 197, n.d.)
[43] (European Maritime Safety Agency , n.d.)
[44] (ESPO: The First Port of Call for European Transport Policy Makers in Brussels, n.d.)
[45] (ILO: International Labour Oeganization, n.d.)

- Customs Trade Partnership Against Terrorism (CTPAT)
- Crew security plan
- Automated Manifest System (AMS)
- SafeSeaNet
- AIS

5.1.3 Cybersecurity standards

5.1.3.1 ISO[46] standards for the security of maritime CIIs

ISO27000 provides definitions of security concepts. ISO/IEC 27001 addresses physical security requirements in terms of preventing unauthorised access to information of an organisation and its relevant facilities which are divided into two broad categories: secure areas and equipment security.

ISO/IEC 27001 also deals with the Information Security Management System (ISMS) of an organisation, which in the case of this report are the CII of the port. Compliance with the ISO 27001 practically means that the organisation, in our case the port, meets the standard's requirements on the security domain which is vital for the well-functioning of the port in a security environment against threats form cyberspace. The CIIs are well protected. Furthermore, it clarifies terms of physical security, such as the physical security perimeter, physical entry controls and facilities. Physical security requirements are identified in NIST special publication 800-171 as well. ISO2800x family of standards provide guidelines for supply chain security and especially for maritime supply chains. The following table[47] summarises the various ISO standards that are relevant to maritime security.

R/N	ISO	COMMENTS
1.	ISO 18788:2015	Management system for private security operations
2.	ISO 9001 / BS 10800	Code of practice for the provision of security services
3.	ISO/IEC 27001	International standard to manage information security
4.	ISO 27002:2013 (previous ISO 17799:2000)	Comprehensive information security standard. It has fourteen sections (5 to 18) each of which is structured in the same way
5.	ISO/IEC TS 30104:2015	Information Technology – Security Techniques – Physical Security Attacks, Mitigation Techniques and Security Requirements
6.	ISO 28000:2007	Specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain
7.	ISO 28000:2022	Security and resilience – Security management systems – Requirements

Since autonomous vessels and innovative maritime applications use AI, various additional standards need to be considered for the development of trustworthy AI-based maritime ecosystem.

[46] (Standards, n.d.)

[47] Y. Papagiannopoulos, "Standards in Practice", IEEE Conference on Standards for Communications and Networking, November, 2022

The main standards for AI are mentioned here below:

5.1.3.2 ISA, ANSI standards for ACS

ISA and ANSI standards are aimed the security of industrial automation and control systems (ACS, .e.g., SCADA). Examples of such standards include:

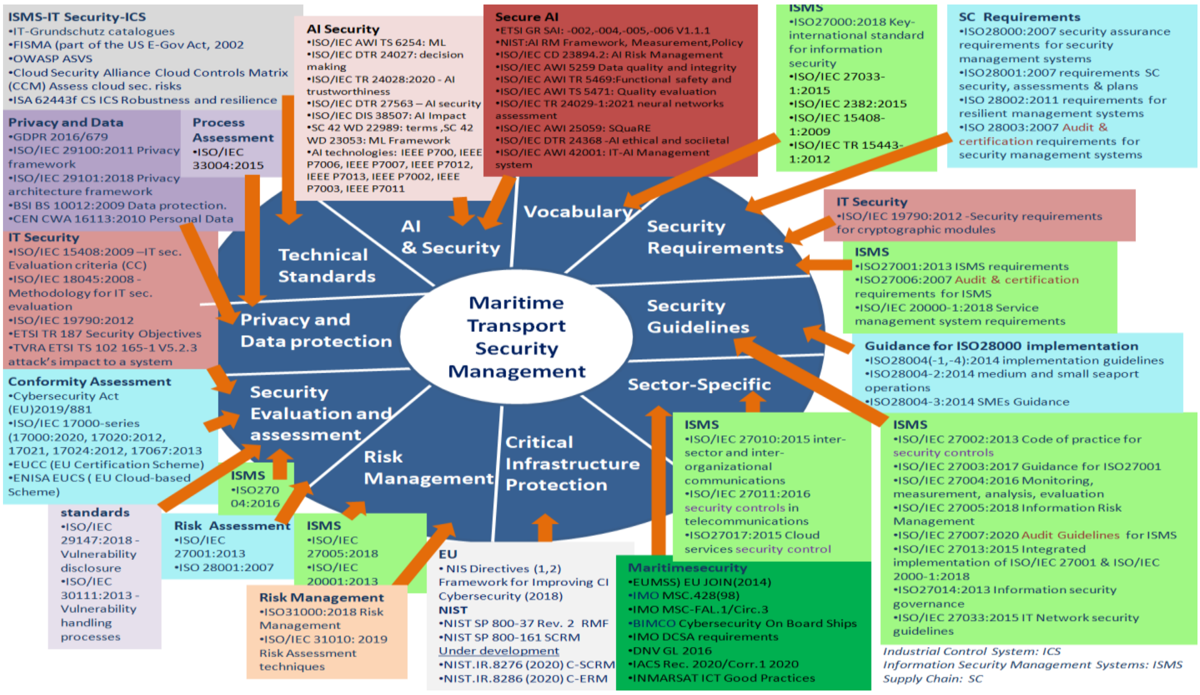
- ISA-TR62443-2-3-2015 Security for industrial automation and control systems, Part 2-3: Patch management in the IACS environment
- ANSI/ISA-62443-2-4-2018 / IEC 62443-2-4:2015+AMD1:2017 Security for industrial automation and control systems, Part 2-4: Security program requirements for IACS service providers (IEC 62443-2-4:2015+AMD1:2017 CSV, IDT)
- ANSI/ISA-62443-3-2-2020 Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design
- ANSI/ISA-62443-4-1-2018 Security for industrial automation and control systems, Part 4-1: Secure product development lifecycle requirements

5.1.3.3 Categorisation of Standards

There are many security standards from various standardisation bodies (e.g., ISO, IMO, ETSI, NIST, BIMCO, IEEE) addressing various topics. These fragmented efforts provide confusion as to which standard(s) to use. Complementarities and overlaps need to be clarified. To contribute to this clarification, a classification of standards[48] has been provided where the following ten categories of standards have been identified:

1. Vocabulary and Conceptualisation: standards that can be used for setting terminologies and description of concepts.
2. Security Requirements: standards setting security requirements.
3. Security Guidelines: standards that provide good practices.
4. Security Evaluation and Assessment: standards and good practices related to assessment or security evaluation methodologies.
5. Privacy and data protection: standards related to the maintenance of privacy and data protection.
6. Risk Management standards: standards and good practices that provide principles, frameworks or processes related to security risk management.
7. Technical standards: standards addressing technical security aspects.
8. AI and security: It includes standards, frameworks and good practices related to AI security (important for the autonomous vessels, maritime drowns).
9. Sector-specific (i.e., Maritime Transport): standards of security management that support the specific requirements and specificities of sector-specific (e.g., port community systems).
10. Critical Infrastructure Protection: standards related to the protection of infrastructures that are critical for the sustainability of the economy and social well-being (e.g., maritime CIIs).

[48] (Kalogeri & Polemi, 2022)


Maritime Transport Security Management
Vocabulary
Security Requirements
Security Guidelines
Sector-Specific
Critical Infrastructure Protection
Risk Management
Security Evaluation and assessment
Privacy and Data protection
Technical Standards
AI & Security

ISMS-IT Security-ICS
- •IT-Grundschutz catalogues
- •FISMA (part of the US E-Gov Act, 2002
- •OWASP ASVS
- •Cloud Security Alliance Cloud Controls Matrix (CCM) Assess cloud sec. risks
- •ISA 62443f CS ICS Robustness and resilience

AI Security
- •ISO/IEC AWI TS 6254: ML
- •ISO/IEC DTR 24027: decision making
- •ISO/IEC TR 24028:2020 - AI trustworthiness
- •ISO/IEC DTR 27563 – AI security
- •ISO/IEC DIS 38507: AI Impact
- •SC 42 WD 22989: terms ,SC 42 WD 23053: ML Framework
- •AI technologies: IEEE P700, IEEE P7006, IEEE P7007, IEEE P7012, IEEE P7013, IEEE P7002, IEEE P7003, IEEE P7011

Secure AI
- •ETSI GR SAI: -002,-004,-005,-006 V1.1.1
- •NIST:AI RM Framework, Measurement,Policy
- •ISO/IEC CD 23894.2: AI Risk Management
- •ISO/IEC AWI 5259 Data quality and integrity
- •ISO/IEC AWI TR 5469:Functional safety and
- •ISO/IEC AWI TS 5471: Quality evaluation
- •ISO/IEC TR 24029-1:2021 neural networks assessment
- •ISO/IEC AWI 25059: SQuaRE
- •ISO/IEC DTR 24368 -AI ethical and socieital
- •ISO/IEC AWI 42001: IT-AI Management system

ISMS
- •ISO27000:2018 Key-international standard for information security
- •ISO/IEC 27033-1:2015
- •ISO/IEC 2382:2015
- •ISO/IEC 15408-1:2009
- •ISO/IEC TR 15443-1:2012

SC Requirements
- •ISO28000:2007 security assurance requirements for security management systems
- •ISO28001:2007 requirements SC security, assessments & plans
- •ISO 28002:2011 requirements for resilient management systems
- •ISO 28003:2007 Audit & certification requirements for security management systems

Privacy and Data
- •GDPR 2016/679
- •ISO/IEC 29100:2011 Privacy framework
- •ISO/IEC 29101:2018 Privacy architecture framework
- •BSI BS 10012:2009 Data protection.
- •CEN CWA 16113:2010 Personal Data

Process Assessment
- •ISO/IEC 33004:2015

IT Security
- •ISO/IEC 15408:2009 –IT sec. Evaluation criteria (CC)
- •ISO/IEC 18045:2008 - Methodology for IT sec. evaluation
- •ISO/IEC 19790:2012
- •ETSI TR 187 Security Objectives
- •TVRA ETSI TS 102 165-1 V5.2.3 attack's impact to a system

IT Security
- •ISO/IEC 19790:2012 -Security requirements for cryptographic modules

ISMS
- •ISO27001:2013 ISMS requirements
- •ISO27006:2007 Audit & certification requirements for ISMS
- •ISO/IEC 20000-1:2018 Service management system requirements

Guidance for ISO28000 implementation
- •ISO28004(-1,-4):2014 implementation guidelines
- •ISO28004-2:2014 medium and small seaport operations
- •ISO28004-3:2014 SMEs Guidance

Conformity Assessment
- •Cybersecurity Act (EU)2019/881
- •ISO/IEC 17000-series (17000:2020, 17020:2012, 17021, 17024:2012, 17067:2013
- •EUCC (EU Certification Scheme)
- •ENISA EUCS (EU Cloud-based Scheme)

ISMS
- •ISO27004:2016

standards
- •ISO/IEC 29147:2018 - Vulnerability disclosure
- •ISO/IEC 30111:2013 - Vulnerability handling processes

Risk Assessment
- •ISO/IEC 27001:2013
- •ISO 28001:2007

ISMS
- •ISO/IEC 27005:2018
- •ISO/IEC 20001:2013

Risk Management
- •ISO31000:2018 Risk Management
- •ISO/IEC 31010: 2019 Risk Assessment techniques

EU
- • NIS Directives (1,2) Framework for Improving CI Cybersecurity (2018)

NIST
- •NIST SP 800-37 Rev. 2 RMF
- •NIST SP 800-161 SCRM

Under development
- •NIST.IR.8276 (2020) C-SCRM
- •NIST.IR.8286 (2020) C-ERM

Maritimesecurity
- •EUMSS) EU JOIN(2014)
- •IMO MSC.428(98)
- •IMO MSC-FAL.1/Circ.3
- •BIMCO Cybersecurity On Board Ships
- •IMO DCSA requirements
- •DNV GL 2016
- •IACS Rec. 2020/Corr.1 2020
- •INMARSAT ICT Good Practices

ISMS
- •ISO/IEC 27010:2015 inter-sector and inter-organizational communications
- •ISO/IEC 27011:2016 security controls in telecommunications
- •ISO27017:2015 Cloud services security control

ISMS
- •ISO/IEC 27002:2013 Code of practice for security controls
- •ISO/IEC 27003:2017 Guidance for ISO27001
- •ISO/IEC 27004:2016 Monitoring, measurement, analysis, evaluation
- •ISO/IEC 27005:2018 Information Risk Management
- •ISO/IEC 27007:2020 Audit Guidelines for ISMS
- •ISO/IEC 27013:2015 Integrated implementation of ISO/IEC 27001 & ISO/IEC 2000-1:2018
- •ISO27014:2013 Information security governance
- •ISO/IEC 27033:2015 IT Network security guidelines

Industrial Control System: ICS
Information Security Management Systems: ISMS
Supply Chain: SC

Figure 8: Taxonomy of security maritime standards[49]

5.2 Safety Legislation

Safety regulations in ports worldwide (including the African) are in principle not fully regulated by international standards and remain the decision of the sovereign state. Each country has established its own safety regulations, which has produced a varied portfolio of sometimes different and outdated laws.

Port governance safety principles are critical as it involves many decision-makers and stakeholders such as the port authority, terminal operators, rail operators, trucking companies, logistics providers and emergency departments. The general safety aspects within the port area, but also the safety aspects of handling cargo are to be considered when developing a port safety management system. It would not be possible to do the subject justice here, but a common factor is that safety must cover qualitative infrastructure and handling equipment, well trained personnel, a set of well thought over procedures and a SMS that monitors and follows-up the actual safety situation. It is the responsibility of the accountable of the port and the facilities to govern their SMS professionally to prevent damage or harm to people. The safety shield should not become fragile, allowing consequential damages from cyberattacks or security attacks.

Most legislation in the maritime world has been initiated by some shipping disaster, and in this case, the Titanic disaster led to the 1974 international safety regulation SOLAS as a protective "safety shield" for seafarers and ships. The extensive media coverage, the subsequent global shock caused by the huge death toll, and the survivors' lawsuit against the White Star Line led to significant improvements in safety at sea.

[49] *Ibid.*

In addition to this social pressure, maritime insurance companies forced shipping companies to show more leadership in preventing accidents and convinced governments to establish more efficient safety laws. There was a shift from running behind the facts, and paying for damages, towards a safety awareness and prevention mentality, which is vital to safeguard humans, cheaper for insurance companies and more efficient for shipowners. The maritime world remains a high-risk industry with huge consequences when something goes wrong.

The most important improvement was the creation of the SOLAS by establishing uniform principles and rules for the construction, installation, and operation of merchant ships. The current 1974 SOLAS version[50] is still the global standard today for ships and seafarers. Each country, each port and each local situation is different and demands for a complex and customised risk approach for all operations to mitigate and minimise safety risks. Some countries, such as Australia, promote the personalised safety leadership approach within ports and merely provide guidance on good practice and outline a template against which the policies, procedures and performance of port operations can be measured.

As each port has its unique safety hazards, safety management rules can only be addressed from within the port itself and use the regulations, guidelines, and international best practice as a tool to improve the safety in the port. A single uniform international safety regulation is not possible in today's world, especially because some countries lack even the basics of safety. But unlike this safety regulation, the creation of a "security legislation" was triggered by a disaster on land, when hijacked aircraft flew into the twin towers of the World Trade Centre on September 11, 2001.

The maritime industry nowadays is controlled by several regulations that require maritime operators to ensure ship safety and security. These regulations also apply to cybersecurity, and with IMO Resolution MSC.428(98). Cybersecurity risks must now be addressed in the Safety Management System (SMS). According to the IMO Maritime Cyber Risk Management Guidelines (MSC-FAL.1 Circ.3), [51] "…maritime cyber risk refers to a measure of the extent to which a technology facility is threatened by a potential circumstance or event, which could result in shipping-related operational, safety or security failures due to damage, loss or compromise of information systems."

In addition to the IMO guidelines, the International Association of Ports and Harbors (IAPH) has also produced a set of cybersecurity guidelines for ports and port facilities.[52]

Some of the specific European port safety regulations involved are:

- Directive 2000/59/EC of the European Parliament and of the Council of 27 November 2000 on port reception facilities for ship-generated waste and cargo residues.

[50] (International Convention for the Safety of Life at Sea (SOLAS), 1974, n.d.)

[51] (Guidelines on Maritime Cyber Risk Management, 2017)

[52] (Measures to Enhance Maritime Security: IAPH Cybersecurity Guidelines for Ports and Port Facilities, 2021)

- Directive 2001/96/EC of the European Parliament and of the Council of 4 December 2001 establishing harmonised requirements and procedures for the safe loading and unloading of bulk carriers.
- Directive 2000/59/EC of the European Parliament and of the Council of 27 November 2000 on port reception facilities for ship-generated waste and cargo residues.

5.3 Cybersecurity Legislation

The EU has adopted and enhanced the ISPS Code with two directives – the EC / 725 /2004 for the Port Facilities and the EC / 65 / 2005 for the Ports. The EU is protecting its infrastructures (including the maritime CIIs) by various legal instruments including:

The *NIS Directive* established a European competence in cybersecurity to protect the digital single market; it has three main objectives: a) improving national cybersecurity capabilities, through requiring all Member States to have a common minimum baseline set of capabilities. This includes adequately resourced Computer Security Incident Response Teams (CSIRTs). b) Facilitating cross-border cooperation at EU-level between Member States and the Union at both strategic/policy and operational cybersecurity levels. This involves both the NIS Cooperation Group and the CSIRTs Network. And c), promoting a culture of risk management and incident reporting among key economic actors, notably Operators providing Essential Services (OES) for the maintenance of economic and societal activities and Digital Service Providers (DSP).

The *EU Cybersecurity Act* establishes a cybersecurity certification framework for products and services. This framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards, and procedures. This way it will be possible to ensure the public trust in the cybersecurity of IT products and services. It is important that it can be shown that a product has been checked and certified to conform to high cybersecurity standards. AI-related products will gain trustworthiness if they are certified and, in the years to come, various cybersecurity schemes will be developed for AI products specifying the security requirements.

The *General Data Protection Regulation (GDPR*) sets data protection rules explaining what, how and when people can access information about them and provides constraints on what organisations can do with personal data.

The *New Legislative Framework (NLF)* improves market surveillance, introduces rules to better protect both consumers and professionals from unsafe products (EU or non-EU), sets rules for the accreditation, establishes a common legal framework for industrial products. NLF will enhance the security of AI-based products.

The *Chips Act* is relevant to AI security because semiconductors are the platform technology of the 21st century that will be used for AI developments and for embedding strong security measures. The globalised EU semiconductor industry will be supported with this proposed Act.

The *Cyber Resilience Act* will set new cybersecurity rules in due time for digital products and ancillary services. This initiative will promote the security of AI products as well since it aims to address market needs and protect consumers from insecure products by introducing common cybersecurity rules for manufacturers and vendors of tangible and intangible digital products.

6 Maritime Security Good Practices

6.1 Introduction

The maritime CIs (ports or ships) need to be considered as physical-cyber infrastructures. There are various guidelines for security the maritime CIs:

- **ENISA Good practices for cybersecurity in the maritime sector** (2019)
- **ETSI TR 103 456** CYBER; Implementation of the NIS **COM(2017) 476 final** "Making the most of NIS"
- **C(2017)6100 final** Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (blueprint)
- **The Tanker Management/ Self-Assessment – TMSA** (OCIMF)
- **The Guidelines on Cyber Security Onboard Ships** (supported by: **BIMCO**, CLIA, **ICS**, INTERCARGO, INTERTANKO, OCIMF and IUMI)
- **Cyber Security Awareness** – AMMITEC

This chapter underlines the steps that need to be followed at a personal, organisational, and operational level to holistically address the security challenges. Security is considered as a joint responsibility and all stakeholders involved need to adopt good cybersecurity practices. Two questionnaires have been developed (see Annexes A and B) to be distributed in the future to maritime operators to capture their security awareness level.

6.2 Maritime Security Governance

The security hygiene of a maritime CI (e.g., port, ship, maritime company) is an integral part of the overall structure of the CI. The security hygiene is all these actions that need to be taken so the maritime CI can function in an acceptable level of risk against physical, cyber, hybrid and supply chain threats. To better understand the security hygiene of a maritime CI, it must first be understood who are the main authorities and stakeholders engaging in the overall structure, operations, services, internal and external users. It is also necessary to identify all physical and cyber assets of the maritime CI, their interconnections, their interplay, and their importance (value) to the operations of the CI. An owner needs to be assigned to every asset that will be responsible for its security (an owner can be responsible for multiple assets).

A maritime CI is a system-of-systems integrated in one entity. To understand better the ecosystem of the CI it is necessary to understand who is engaging in the asset management. This is important since it indicates the information security governance of a maritime CI and the overall security measures that need to be taken to protect these assets.

Every Maritime CI needs to apply and practice an information security governance schema as follows:

- Policies (mandatory)

- Standards (mandatory)
- Guidelines (non-mandatory)
- Procedures (mandatory)
- Baselines (mandatory)

The policies, standards, guidelines, and procedures set up the security governance of an organisation. In this regard, the security hygiene of an organisation can be achieved through implementing the elements of the security governance and to establish a well-protected Information Security Management System (i) based on the appropriate security controls, (ii) implement the security controls (iii) the evaluation of the security controls in the maritime environment that are being applied and (iv) the monitoring of their effectiveness regularly. The security hygiene needs to be applied based on the security governance approach described above.

Governance structure needs to be applied to both aspects of security (safety and cybersecurity) in a uniform approach and needs to be an integral part of all maritime CI activities. Governance procedures need to include a Business Impact Analysis (BIA), an updated Risk Assessment and a Security Policy. In this regard the information security governance needs to be regularly monitored and evaluated based on Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) of the physical and cybersecurity and personnel safety. An incident handling team needs to be part of the security governance team that will be responsible for the forecasting, identification, analysis, mitigation, and recovery of any security incident (physical, cyber, hybrid).

A central Authority need to be established, with a mandate to supervise the implementation of the information security governance by inspecting (conduct security control) the overall security system of the maritime CI.

6.3 Operators' Cybersecurity Hygiene

Data from Verizon's 2019 Data Breach Investigations Report (DBIR) indicates that nearly one-third (32 percent) of all data breaches involved phishing scams.[53] A new phishing site launches every 20 seconds as mentioned in the 2020 Mobile Threat Landscape Report, Wandera. Human error caused 90 percent of cyber data breaches in 2019, according to analysis of data from the UK Information Commissioner's Office (ICO) carried out by CybSafe. According to this analysis, nine out of 10 of the 2376 cyber-breaches reported to the ICO last year were caused by mistakes made by end-users. Phishing attacks account for more than 80 percent of reported security incidents; 17,700 dollars are lost every minute due to phishing attacks; 60 percent of breaches involved vulnerabilities for which a patch was available but not applied by the administrators.

Good personal security practices need to be applied by all maritime operators and individual users by setting the rules and efforts to:

- Build a security culture awareness and cyber hygiene

[53] (Widup, 2019)

- Encourage information sharing and collaboration
- Engage operators and users in the security related decisions and procedures
- Use posters and reminders
- Continuous hands-on security training at all levels (from seminars to exercises)
- Effective access control
- Enforce authentication and password policies

6.4 Maritime Security Management

Management of physical, cyber and hybrid risks require a holistic approach. The general steps that need to be taken during the security (safety and cybersecurity) management of a maritime CI are:

1) Identify the (physical and cyber) assets and assign ownership e.g., assign a person(s) that will be responsible for the asset.
2) Create a dynamic updating inventory of assets (list the ownership).
3) Categorise and classify the assets based upon:
   - Value of the asset (importance for the maritime CI);
   - Importance of the asset in the overall maritime ecosystem;
   - Type of the asset (physical, cyber, user, procedures).
4) Identify threat landscape and attack surface of every asset.
5) Select and use a risk assessment methodology (e.g., from ENISA' inventory)[54] and estimate the risks.
6) Undertake measures to protect the assets using published lists of controls e.g., ISO 27002, NIST2020, SANS Top 20, CIS and best practices and develop the risk treatment plan (contingency plan).
7) Develop the security policy with rules that govern how assets are managed, protected and distributed within the organisation, utilising existing efforts e.g., ISPS, BIMCO guidelines or ISO/IEC PDTR 13335-1 (11/2001).
8) Continuously identify new threats, incidents, assess the risks, ownership of the CII assets, the strength of the controls and the management of the incidents.

[54] (Inventory of Risk Management / Risk Assessment Methods and Tools , n.d.)

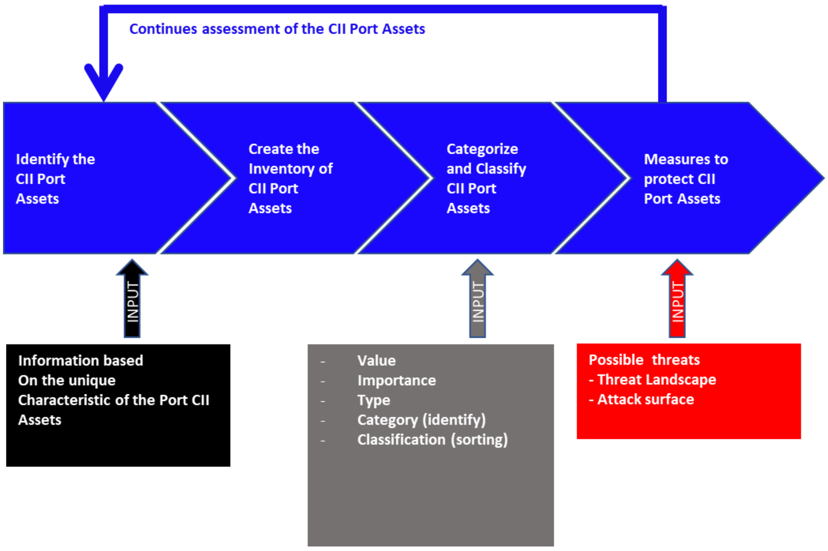

Continues assessment of the CII Port Assets
Identify the CII Port Assets
Create the Inventory of CII Port Assets
Categorize and Classify CII Port Assets
Measures to protect CII Port Assets
INPUT
INPUT
INPUT
Information based On the unique Characteristic of the Port CII Assets
- Value
- Importance
- Type
- Category (identify)
- Classification (sorting)
Possible threats
- Threat Landscape
- Attack surface

Figure 9: BIMCO approach to Security Management

6.4.1 Safety (Physical Security) Management

Prior to the incident of 9/11, merchant ships traditionally entered territorial waters and ports without inspection to facilitate fluid economic trade and avoid ship delays. Only when the ship was at anchor or moored did port authorities, customs, and immigration officials board to clear the ship, crew and cargo. This made the port very vulnerable to being targeted by criminal organisations and terrorist organisations. A terrorist attack on a port could severely impact local populations, port infrastructures, and regional economies dependent on these port activities.

Port safety management regulations and protocols also help prevent accidents, and thus help reduce the severity of injuries if an accident does occur. It is essential because it creates a working environment free of hazards and minimal risks. This improves the quality of terminal operations and the reputation of the port and can be considered a commercial tool to attract more ships.

The IMO was chosen as the most logical organisation to draft a new security code with entry into force on July 1, 2004, the ISPS Code. Initially focused on the physical security (safety) management, it now increasingly highlights cybersecurity risks and, in the future, will also focus on airborne risks (i.e., drone attacks).

In some seaports, however, security problems still occur, allowing safety threats to enter the port and its facilities. This is partly because the implemented national ISPS Code addresses safety measures to be taken in port facilities and not as such in the port area around these terminals or in ports' supply chain business partners/ facilities.

A seaport is a maritime logistics and industrial hub in the global economic supply chain. Port activities such as storage and ship handling are directly or indirectly linked to international transport and information processes involving many actors. This means that many people enter and leave port access via ships, trucks, rail, vehicles or as pedestrians. The COP and the

ISPS Code require that all these movements be monitored to prevent illegal acts. The purpose of this section is not to explain the full ISPS Code or all the details of the Code of Practice on Security in ports, but to understand how these codes can be applied in ports to best resist attacks. All the security measures and daily operating practices below are described in more detail in the PSP and PFSP.

6.4.1.1 Port and Port facility boundaries

Both codes require that all people be checked when entering and leaving the port or a port facility. But what are the administrative boundaries of the facility and, more importantly, of the port to monitor?

Observations show that in some ports, port captains are not sure whether they are the person to be held accountable and final responsible as port authority to act for incidents that happen 90 miles out to sea, or in the bay of the port or on a nearby stretch of beach outside the visual port area. We observed confusion between the port authority and private terminal operators in concluding who is responsible for incidents that happen within the dock water in front of the respective port facility. It is important to include the exact administrative boundaries of the port and each port facility (including the water bound limits) in the Port Security Plan (PSP) and Port Facility Security Plan (PFSP). This allows the most efficient action to be taken and the right people to be contacted in the event of an emergency. Efficient actions prevent consequential damage and ensure rapid restoration of normal economic conditions.

6.4.1.2 Security accountability

Port facilities bear ultimate responsibility for handling ISPS security incidents. This means that the Port Facility Security Officer (PFSO) must act in accordance with the ISPS regulation and the Port Security Officer (PSO) must act in accordance with the guidelines of the COP. It is not the PSO's job to take overall responsibility for risks occurring in port facilities, but to cooperate with the PFSO in that case.

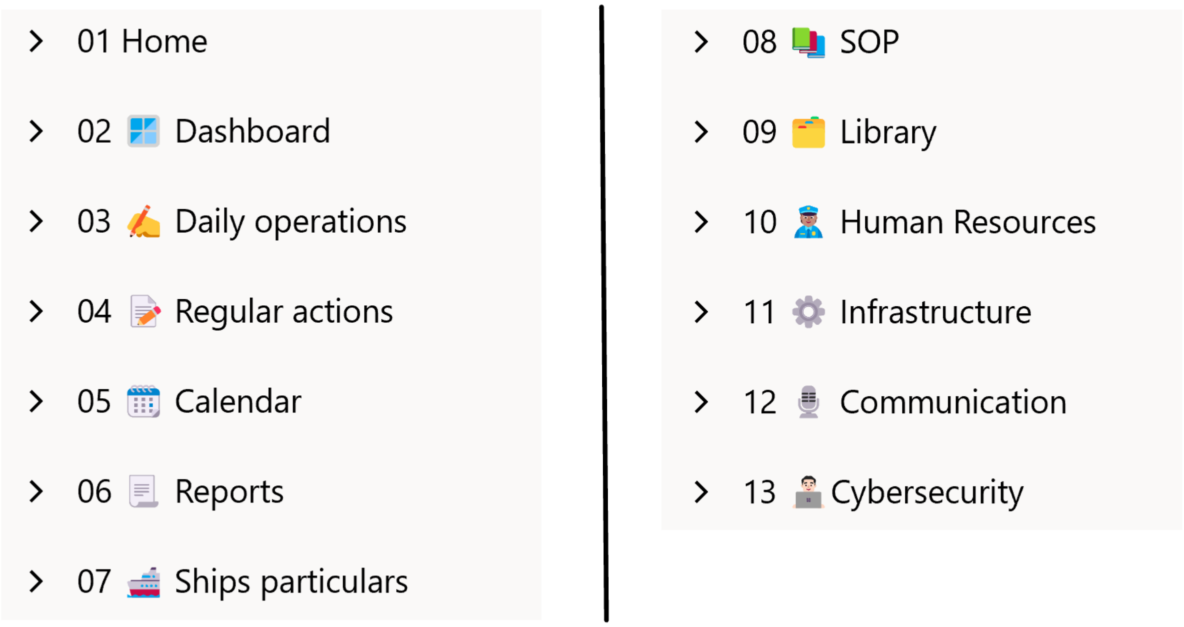
Experience shows that in some countries the ISPS Code has been translated into a national security law that designates the PSO as ultimately responsible for security incidents. This puts the PSO in a situation where the port (rather than the port facility) becomes the final responsible party for ISPS security incidents in port facilities. The result is that security risks remain unresolved because the port is unlikely to invest in security measures within a private port facility concession.

6.4.1.3 The Security Management System (SEMS)

To demonstrate adequate governance, port security departments must be well organised and consider both physical and cyber threats. They must be able to monitor and correct daily security activities and need management tools to do so. With a management system, they can monitor the state of the security infrastructure and the performance of security personnel and verify that all security functions are being properly performed.

In many ports, no SEMS is available. Security officers sometimes act as crisis managers and focus on mitigating incidents rather than preventing them. They should manage all aspects of security and take daily measures to prevent physical, cyber and hybrid incidents. The

Information Security Management System (ISMS), which makes part of the SEMS, is implemented via the compliance with the ISO 27001 requirements.[55] All the CIs of the port need to meet the requirements of the IS0 27001 and manage cyber risks.



› 01 Home
› 02 Dashboard
› 03 Daily operations
› 04 Regular actions
› 05 Calendar
› 06 Reports
› 07 Ships particulars
› 08 SOP
› 09 Library
› 10 Human Resources
› 11 Infrastructure
› 12 Communication
› 13 Cybersecurity

Picture: Example of a SeMS (Christophe Van Maele)

6.4.1.4 Physical security control activities at the gates

Each time a person (on foot or in a vehicle) enters the ISPS facility, that person's identification card (or badge) must be checked before being admitted into the zone. A record of the person and time of entry is required by the code. Once the person leaves the ISPS facility, the time of departure must be recorded. This allows for knowledge of who is in the ISPS zone at all times and can help in the search for a specific person or during an emergency evacuation. Technology can be a great help, as electronic barriers, turnstiles, and digital badge systems eliminate manual error-prone registrations, especially if a facility has multiple entrances and exits.

Reality shows that manual registration is still the norm in many ports. Moreover, manually operated barriers allow access by the guard, who can decide without any review of his/her decision.

If the port acts as the first point of entrance, which is often the case when the port area is a free trade zone, the same security control principles must be applied. Again, many deficiencies are found in practice.

[55] (ISO/IEC 27001 and related standards: Information security management, n.d.)

6.4.1.5 Security control activities within the port area

Mobile security guards run patrols and check that people are allowed into the ISPS area or port area. To make this easier, visible ID badges should be worn by anyone inside the area. However, ID checks are rarely performed, nor do all people visibly wear their badges.

6.4.1.6 Perimeter security control

Perimeter control is the control at the administrative boundaries of the port or port facility. In most cases there are physical barriers, but within the European Union some non-critical terminals, such as general cargo terminals handling sand, are not required to be fenced. They may have a camera system to monitor their boundaries. Perimeter monitoring is often done from a Security Control Centre where operators analyse images and decide what action to take. Their colleagues on the mobile surveillance teams do physical security rounds. It is good practice to use a tag round system to ensure they have checked all tag point areas. Tag rounds are sometimes not performed, and operators could be better trained in many ports.

6.4.1.7 Communication between all security stakeholders

Regular meetings should be organised between PFSOs and the PSO to update each other on the detailed current security situation in the port, discuss potential risks, handle incidents, and keep abreast of new developments in the port. PSOs should hold the same type of meetings at the national level (National Maritime Security Committee) with other stakeholders such as port police, customs, navy, designated authorities, and others. At these meetings, security issues of national attention are discussed, and acute situations are addressed, such as scaling up to security level 2 or 3.

In some countries the various stakeholders stay on their own turf and do not meet regularly or at all. In this case, a coordinated plan of action often does not exist or exists only on paper, leaving room for criminal activities to remain undetected.

6.4.1.8 Capacity building through personnel training

It is vital to have well-trained security personnel who know how to do their jobs. People in ports sometimes change jobs, so, regular training sessions for new recruits and safety rehearsals for security personnel are required. In addition to basic ISPS training, on-the-job training is equally important to understand how to manipulate the often-digitised control room applications and how to act in an emergency.

Training is considered necessary in all ports around the world. It is important to keep training standards high to prevent trained personnel from not being able to respond efficiently to incidents.

6.4.1.9 Security incident handling-management

When the port has implemented proper security management principles, ISPS-compliant port facilities can be considered protected against intentional illegal actions. This includes the above-mentioned preventive principles taken to protect people from theft, vandalism, terrorism, cyberattacks, violence, drugs, and other threats. It is important to understand that, both in regulation and day-to-day management, the ISPS and COP are based on prevention. This means that port security measures are taken in anticipation of potential threats before they occur. These measures are designed to deter criminals and reduce the likelihood of a crime or act of violence. Mandatory ISPS security assessments (Privacy and Security Assessment process (PSA)/Port Facility Security Assessment (PFSA)) and security plans (PSP / PFSP) form the basis for this state of compliance.

Should a security incident nonetheless occur, the role the port plays can change. Scaling up to a higher ISPS security level is the decision of the designated authority. In that case, a strategic crisis team is assembled, and law enforcement agencies are called in to deal with the acute situation; thus, the port generally does not decide by itself which immediate proactive security measures to take. Long-term measures are proposed by the port (facility), approved by the designated authority, included in the port security plan (facility), and only then implemented.

IT and OT systems are also in constant use. Within the security domain of ports and ISPS-compliant terminals, it is necessary to consider the following:

- the SEMS security management system is efficient only if it is digitised
- the ID badge system is efficient when it is a digital system based on a common database to which law enforcement and customs also have access
- the automatic barrier system admits only persons entitled to enter the zone
- a perimeter monitoring system with a high-performing CCTV or other camera system will take smart actions and can track video footage for long periods of time
- the use of computers to communicate between stakeholders enables real-time and efficient action when needed. Information systems nevertheless remain the domain of the IT department

To date, several of these security systems have not been installed in ports covered by the study. Consequently, these ports could not be attacked by cyber-terrorists with respect to these systems. This type of risk will only occur once the security systems in these ports are digitised.

6.4.1.10 Information system control

As more and more day-to-day security operations are digitised, there is a large amount of information that needs to be shared and protected. This is described in more detail in the chapter on cybersecurity.

6.4.1.11 Ships Security Management

The ISPS Code applies to port facilities and aboard ships. Although the same code applies to both areas, there are several aspects that apply only aboard a ship. Should a terrorist gain control of a ship, cargo, crew and information system, this could cripple a port for a long time. The Ship Security Officer (SSO) is responsible for the proper management of security onboard in accordance with the ISPS Code to prevent pirate attacks and hijackings of ships. They are supervised by their Company Security Officer (CSO). The management principles correspond to those within the port.

To be prepared for external threats, the IMO has taken the initiative to help ships with guidelines to prevent attacks. A ship must be able to withstand an external attack through ship protection guidelines. The implementation of these protection measures is divided into a first level of defence, a second level of protection and a final layer.

- The first level of defence protects the ship from being boarded by attackers. This includes vigilant lookout teams, searchlights, manoeuvring the ship away from attackers, barbed wire and water sprinklers and, in some instances, private armed guards.
- The second level of defence takes effect once the attackers are on board and is designed to protect the bridge and access to the castle. This can be done through door locks, motion sensors, CCTV systems and a vigilant crew.
- The third level of defence is activated if the attackers take over the bridge and gain access to the information system. In that case, the crew can hide in a purpose-built bunker called Citadel, where vital engine and steering controls are available, and the communications system can be monitored.

The crew must fully understand how everything works in the Citadel and what the important means are to keep control of the ship from there. If they are not properly trained to control the ship from this bunker space, the Citadel itself can become a fatal prison for the crew gathered there for own protection.

6.4.2 Cybersecurity Management

The cybersecurity management model developed by BIMCO[56] (based on the NIST Risk Management Framework (RMF))[57] follows the general security assessment steps described in Section 6.4 and contains the following components regarding the cyber risk management:

1. Identify threats
2. Identify vulnerabilities
3. Assess risk exposure (risk estimation)
4. Develop protection and detection measures
5. Establish contingency plans
6. Respond to and recover from cybersecurity incidents

The most crucial point when dealing with the cybersecurity is to identify the threat landscape which practically means identifying what the possible threats are that may affect maritime CI assets. Some examples of cyber threats that were identified during the year 2020 by ENISA[58] are: (1) Malware, (2) Web-based attacks (3) Phishing, (4) Web application attacks, (5) Spam, (6) DDoS, (7) Identity theft, (8) Data breach, (9) Insider threat, (10) Botnets, (11) Physical manipulation, damage, theft and loss, (12) Information leakage, (13) Ransomware, (14) Cyberespionage, (15) Crypto jacking.

As soon as the threat landscape is identified, the attack surface – the set of all attacks that can be used to exploit threats – of the CI assets can be easily identified (point 4 in paragraph

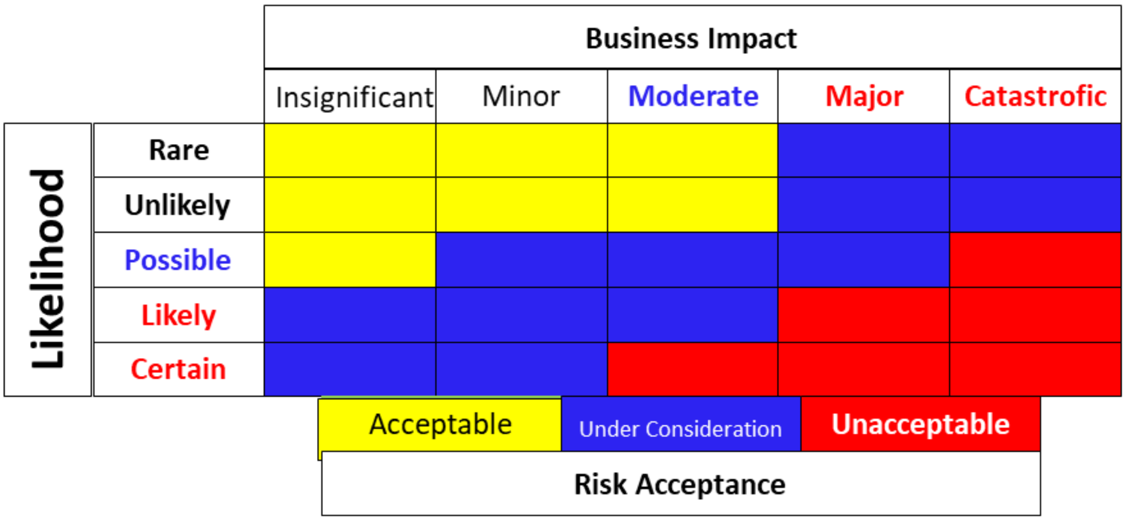
[56] (The Guidelines on Cyber Security onboard Ships - Version 4, 2020)
[57] (NIST Risk Management Framework (RMF), n.d.)
[58] (European Union Agency for Cybersecurity (ENISA), 2020)

6.4 above). The attack surface of these assets can be derived based on their vulnerabilities, and thus a vulnerability assessment needs to take place.

The next step identified in BIMCO is to assess the risk exposure regarding the CI Assets. In particular, the risk is split into four types of risk response, i.e., to:

- *avoid the risk*: in this case the risk is not accepted (a decision by the top management of the port needs to be taken upon recommendation by the Chief Information Security Officer (CISO))
- *transfer the risk* (i.e., to an insurance company): a decision by the top management of the port also needs to be taken upon recommendation by the CISO since it might have financial impact
- *take mitigating actions*: to mitigate the risk is also a decision needed to be taken by the top management of the port upon recommendation by the CISO since it might also have financial impact
- *risk is accepted*: the acceptance of the risk it is a direct business decision and only the top management can take this decision.

To mitigate the risk, protection and detection measures need to be developed and a response plan needs to be established to bring the risk to an acceptable level. The acceptable level is defined by the maritime CI (**risk appetite**) after conducting a cost-benefit analysis or after identifying the business impact of the risk. The **risk appetite matrix** describes a qualitative risk analysis:



		Business Impact				
		Insignificant	Minor	Moderate	Major	Catastrofic
Likelihood	Rare	🟨	🟨	🟨	🟦	🟦
	Unlikely	🟨	🟨	🟨	🟦	🟦
	Possible	🟨	🟦	🟦	🟦	🟥
	Likely	🟦	🟦	🟦	🟥	🟥
	Certain	🟦	🟦	🟥	🟥	🟥

Risk Acceptance		
🟨 Acceptable	🟦 Under Consideration	🟥 Unacceptable

Figure 10: Risk Appetite Matrix

If the mitigating measures cannot bring the risk up to an acceptable level according to the risk appetite matrix, then a business decision needs to be taken by the top management of the port to either accept the risk or not.

The risks need to be assessed on a case-by-case basis according to the cyber ecosystem of the

CI and accordingly need to be defined as (i) acceptable (ii) risks to be discussed (mitigating measures or risk transferred) (iii) unacceptable, need to be avoided.

The BIMCO Guidelines on cybersecurity onboard ships are based on high-level principles:

- establishment of awareness of the safety, security and commercial risks that present themselves due to a lack of cybersecurity measures;
- protection of shipboard IT infrastructure and connected equipment;
- system for authentication and authorization of users, to ensure appropriate access to necessary information;
- protection of data that is used in the ship environment, ensuring it has adequate protection based on the sensitivity of the information.

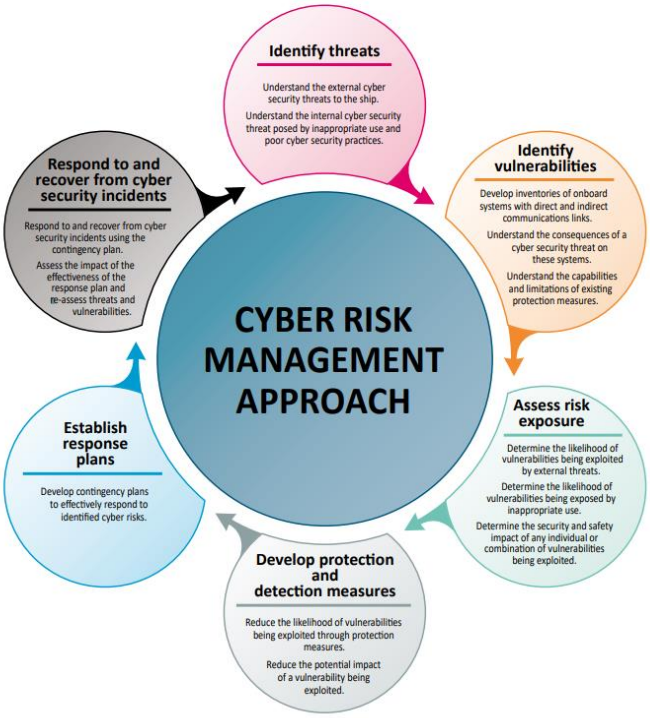

Identify threats
Understand the external cyber security threats to the ship.
Understand the internal cyber security threat posed by inappropriate use and poor cyber security practices.
Identify vulnerabilities
Develop inventories of onboard systems with direct and indirect communications links.
Understand the consequences of a cyber security threat on these systems.
Understand the capabilities and limitations of existing protection measures.
Assess risk exposure
Determine the likelihood of vulnerabilities being exploited by external threats.
Determine the likelihood of vulnerabilities being exposed by inappropriate use.
Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.
Develop protection and detection measures
Reduce the likelihood of vulnerabilities being exploited through protection measures.
Reduce the potential impact of a vulnerability being exploited.
Establish response plans
Develop contingency plans to effectively respond to identified cyber risks.
Respond to and recover from cyber security incidents
Respond to and recover from cyber security incidents using the contingency plan.
Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.
CYBER RISK MANAGEMENT APPROACH

Figure 11: BIMCO Cybersecurity management approach[59]

- management of IT users, to make sure they only have access and rights to the information for which they are authorised;
- management of communication between the ship and the shore side, and
- development and implementation of a cyber incident response plan based on a risk assessment.

The ports' assets value (importance in maritime operations) determines the security requirements and controls that need to be undertaken. Various efforts (e.g., SAURON project) contribute towards classifying the port assets and propose security architectures.

[59] (The Guidelines on Cyber Security onboard Ships - Version 4, 2020)

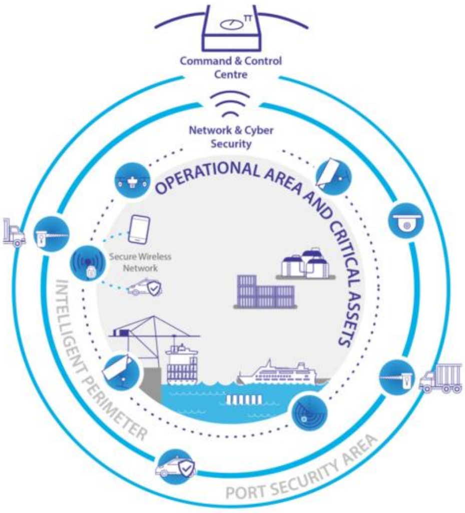


Figure 12: SAURON physical-cyber security architecture[60]

This approach contributes towards the security of the ports ensuring the safety of the physical assets and the cybersecurity of the cyber assets.

6.5 Maritime Cyber Resilience

Maritime cyber resilience[61] is the ability of the maritime CI to resist attacks. Resilience is achieved if the security (safety and cybersecurity) is ensured and if the governance structure is effective and auditable, e.g., the strength of the controls and security procedures (such as disaster recovery procedures) are regularly tested.

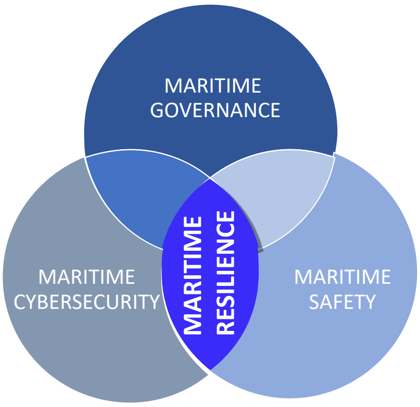


Figure 13: Maritime Resilience

[60] (Company, 2017); (Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports, n.d.)
[61] (Erstad, Ostnes, & Lund, 2021)

Various organisations adopt a more general view of security, e.g., according to the Institution of Engineering and Technology (IET),[62] security strives to attain and maintain eight general security objectives as shown below:

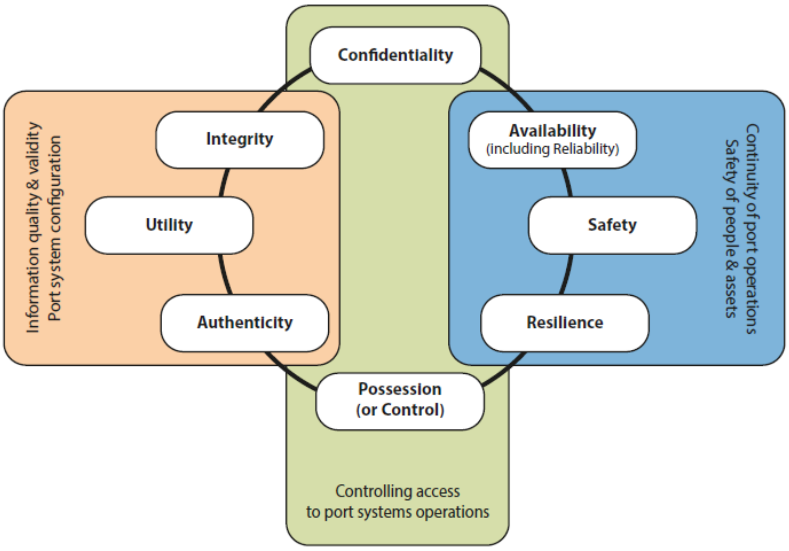

Confidentiality
Integrity
Utility
Authenticity
Information quality & validity
Port system configuration
Availability
(including Reliability)
Safety
Resilience
Continuity of port operations
Safety of people & assets
Possession
(or Control)
Controlling access
to port systems operations

Figure 14: IET Security Objectives

6.6 Human Factors

The human nature, behaviour, social, cultural, and ethical values make the individual the prime enabler of the cybersecurity attacks or a skilled cybersecurity defender or a security aware maritime operator and officer. Human profiles and their characteristics play a major role in future advancements in securing maritime assets and infrastructures.

Investigating human factors and parameters of the members of the ports and ships security teams or by studying the profiles of attackers (from past security incidents) helps forecast or prevent an incident and more effectively manage an attack.

Furthermore, by identifying the profiles of the maritime personnel (e.g., operators, agents, administrators, crew members), the maritime CI may develop more effective security training addressing their needs and their security comprehension levels. Security plans and procedures need to be clear for all employees in order to use and embrace[63] them daily. The development of applicable security procedures requires involving the employees in the development of these procedures.

[62] (Good Practice Guide: Cyber Security for Ports and Port Systems, 2020)

[63] (Kioskli & Polemi, Psychosocial Approach to Cyber Threat Intelligence, 2020); (Kioskli & Polemi, A Socio-Technical Approach to Cyber-Risk Assessment, 2020)

The human factor is the turning point in the overall security of the maritime ecosystem. Usually, ports and ships are the weakest links in the security chain compromising the maritime operations and services despite the technological means that are in place; people are the biggest threat.

The security awareness of the maritime stakeholders needs to continuously be monitored; distributing and analysing the questionnaires found in the Annex may contribute towards this need. Awareness raising campaigns and targeted practical training are the means to prepare maritime employees and stakeholders in becoming the main security guards and defenders of physical and cyber-attacks in the maritime ecosystem and enhance the security maritime culture.

7 Ports Security Practices in Africa

7.1 The Gulf of Guinea ports

Around 1500 ships per day (tankers, cargo vessels and fishing vessels) navigate in the waters in the Gulf of Guinea addressing 20 major ports. This important economic flow creates a golden opportunity for piracy and kidnapping of seafarers, armed robbery at sea, illegal fishing, smuggling and human trafficking in and around ports, and transnational organised crime and terrorist attacks. It poses a major threat to maritime security for all vessels attending these ports and ultimately to the economic development of the countries within the entire region.

The economic potential in the Gulf of Guinea region is expected to increase further in the coming years but before it can realise and benefit from this potential, threats to its stability and prosperity must first be addressed. This requires the continuous identification and addressing of security challenges linked to the sea, the seaports and the hinterland.

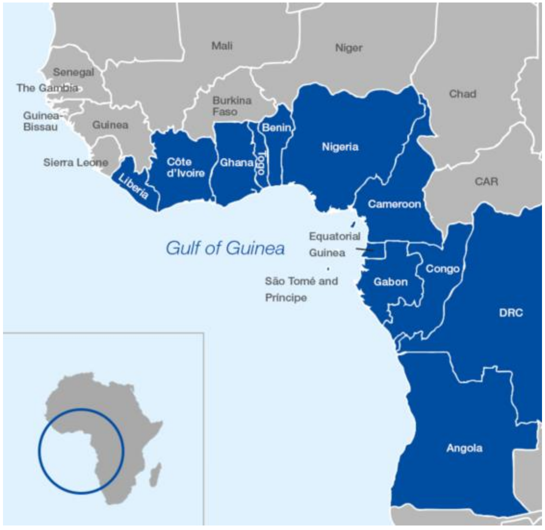


Figure 15: Gulf of Guinea Maritime Region[64]

7.2 Organisation of Port Security in Africa

Seaports in Africa are organised in the same way as other ports around the world. The port authority is run in its day-to-day operations by state officials, who are accountable to their respective ministries.

A Port Authority has several departments. One of the departments is the IT department and another is the Operations department, which is headed by the Port Captain. Observations in ports worldwide showed that the Port Captain is appointed as the overall responsible, aside nautical operations, for security within the port and facilities operated by the port itself. The security department must implement ISPS regulations in the port and enforce the security shield. The port safety department, on the other hand, focusses on human safety and almost

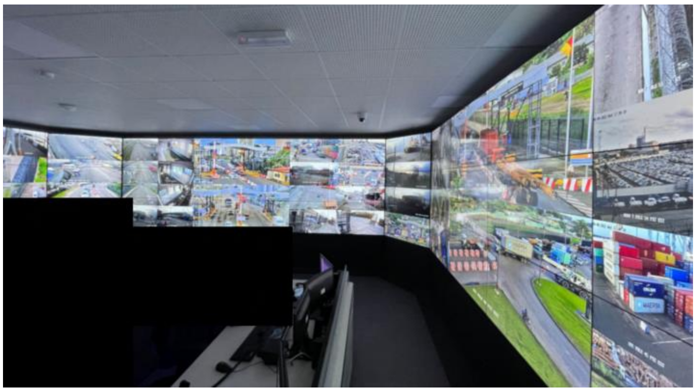
[64] (Gulf of Guinea Map, 2021)

always maintains an intervention team that acts in case of fire and first aid. At the administrative level, the port IT department provides cybersecurity rules related to general administrative port systems, but the ISPS security infrastructure is often outside their scope and is done by the external companies that installed the security hardware. Ports receive revenue based on the vessel cargo volume of their shipping customers through the "ISPS surcharge". This fee covers the cost of the comprehensive set of measures to improve ISPS security of port facilities.

An example of a good security practice includes the following IT architecture:

There are 4 main OT and IT security systems that are crucial to prevent a security incident. If any of these systems is attacked by a cyber-attack, the physical security integrity of the port is compromised.

- The first system is the *OT badge system*: A badge system is based on a digital database of people doing business at the port. The database consists of port staff, dock workers, truck drivers, customers, and visitors. After an initial administrative person check (by police) when applying for a badge, the person is allowed into the port on certain days and at certain times. At best, the database is checked regularly by the police, who can block persons with nefarious intentions. A badge system will be installed by an external security company, which has admin rights to maintain the OT system. Port security personnel produce and distribute the badges. If the badge system is hacked and access time is extended, a criminal can receive a port badge and enter the port area undetected.
- The second security system is the *OT access control system*: This system allows persons to enter the port (and port facility) premises when they show their badge within the authorised time frame. The access control system accesses the badge database and decides whether to open gates, doors, turnstiles, access barriers, etc. The access control system is usually installed by the same security integrator as the badge system. If the access control system can be misled by a cyber-attack, criminals (and their contraband) have free access in and out of the port.
- The third system is the *OT perimeter control system*: To control the port perimeter, there is a need for fencing and a monitoring system to control illegal entry. Nowadays, CCTV systems as well as thermal and infrared camera systems are used in civilian ports and port facilities to check the integrity of the fence. Moreover, a security control room is built to monitor and act in case of intrusion and breach. These camera systems are installed by specialised external companies that have administrative rights on the system. The cameras are operated by port security personnel. If the camera system were to be hacked by a cyber-attack, guards could be misled and shown false images, allowing illegal entry or theft through the perimeter fences.



[redacted]

Figure 16: OT perimeter control system[65]

- The fourth system is the *IT system*: The IT system used by security personnel mainly consists of a security management system SeMS, digital office documents, e-mail, and Internet connection. This system is installed by the port's IT department, who retain administrative control of the cybersecurity shield. If the operators are lured into a cyber-attack, by using an infected USB stick, for example, communication between the security guards could be impeded, resulting in a blind security situation.

In other ports in South and East Africa, the same security principles are applied as in the Gulf of Guinea ports. Private port operators holding port facilities under concession organise themselves to be safe and ISPS-compliant.

Port authorities focus on keeping the common port area safe and secure within the administrative port boundaries. They take measures to protect this area from the anchorage zone, mooring zones, up to port docks and the entire port area (exclusive private areas).

7.3 International Initiatives for African Ports

There are several projects focussed mainly on improving security on the open seas, piracy, cross border actions and drugs:

- The USA is present with its U.S. Africa Command (AFRICOM) program, focusing on high sea securing initiatives by warships and support for local navies.
- Countries in and around the Gulf of Guinea signed the “Code of Conduct concerning the Repression of Piracy, Armed Robbery against Ships, and Illicit Maritime Activity in West and Central Africa” (the Yaoundé Code of Conduct). This Yaoundé architecture promotes regional maritime cooperation and safeguards a stable maritime environment.
- Europe is present with the Critical Maritime Routes (CMR) programme. A set of projects focussed on legal framework, operational rules, information sharing, training, and capacity building.
- The Gulf of Guinea Inter-Regional Network (GoGIN) aims to enhance maritime domain awareness the Yaoundé Architecture Regional Information Sharing network (YARIS).

[65] Photo taken by Christophe Van Maele

- Support to West Africa Integrated Maritime Security (SWAIMS) aims to improve law enforcement and governance frameworks.
- Support Program to the Maritime Security Strategy in Central Africa (PASSMAR), focuses on cross-border maritime cooperation.
- Seaport Cooperation Project (SEACOP) seeks to build capacities and strengthen cooperation against maritime illicit trafficking.
- International organisations such as Interpol and UNODC's Criminal Network Global Disruption Programme (CRIMJUST) are focusing on drug trafficking routes.

It is the sole decision of the country how to deal with security and cybersecurity in ports and international involvement has to have national approval.

- West and Central Africa Port Security project (WeCAPS),[66] a project of the CMR in the Gulf of Guinea region) aims to improve port security and to comply with the ISPS. This project analyses the risks within 10 ports in the Gulf of Guinea region and executes safety actions regarding personnel training, expert advice and implementing SeMS.
- IMO[67] and the United States Coast Guard (USCG)[68] have an important role in ISPS bound seaports and are present with several training activities, improvement visits and assistance projects in African ports.

7.4 Cyber Risks in Africa

With the increasing digitalisation of the maritime industry and the increasing power of the tools at the disposal of cyber criminals, the number of cyber-attacks has increased, including attacks on ships, and approaching seaports. Although most maritime cybersecurity incidents to date have not targeted African ports, available evidence of cyber-attacks in other sectors and ports elsewhere in the world help provide valuable information for African governments and port authorities.

These cyber-attacks would pose an existential threat to the economy of the African continent if ports were to be attacked. A recent Institute for Security Studies report[69] on African cybersecurity in the maritime world shows how cybersecurity is fast becoming an important aspect of African maritime security needs as digitalisation takes hold in Africa's maritime industry. With current technological changes on ships, African ports will need to increase their cybersecurity shield to remain competitive. African ports need to think differently about threats, risks, and vulnerabilities, as well as criminal actions.

Ships are leading the way in addressing cybersecurity measures and are required to include cybersecurity measures in their ISM manual and are challenged by the IMO and their insurance companies to take cybersecurity seriously. In contrast to shipboard initiatives, there remain security and cybersecurity challenges in Sub-Saharan African seaports to improve their shield.

[66] (WeCAPS, n.d.)
[67] (Our Work, n.d.)
[68] (Atlantic Area Units, n.d.)
[69] (Reva, 2020)

A noteworthy cyber-attack took place in July 2021 when Transnet, a major South African port company, which handles 60 percent of the country's container traffic at the port of Durban (South Africa), was hit by a ransomware attack. This caused massive disruption. Their container terminals in Durban, Ngqura, Port Elizabeth and Cape Town had to switch to manual processing of cargo until the IT systems were restored. The result was a huge congestion of more than 14 hours for trucks to pick up and unload containers and the inevitable loss of revenue for the terminal operator. ISS predicted in the same report that incidents like the Transnet attack will increase across Sub-Sahara Africa, as seaports are attractive targets, still vulnerable to cyber-attacks. In this case, transport infrastructure, especially a port, is a lucrative target for cyber criminals or other hostile actors because of the scale of operations and high international media impact.

Although major Sub-Saharan African ports have IT systems departments, implementation and compliance with concrete cybersecurity measures are far from being achieved, and this situation poses a clear security risk. Port policymakers understand that progress needs to be made and show great interest in improving the cybersecurity shield within their operations and security systems, such as CCTV systems, badge systems and access control systems. But the same port authorities do not have enough knowledge to improve their cyber resilience and there seems to be few awareness campaigns lead by national policymakers towards ports to reduce cyber risks. There are not many cyber protocols observed in port security departments.[70]

One of the EC projects in the Gulf of Guinea (WeCAPS) has taken the initiative to ensure that port staff at different levels are aware of cyber threats and associated risks and are able to act accordingly. It focusses on awareness training for operators and staff and would have carried out more improvement actions on the infrastructure side (access systems, badge systems, CCTV systems and communication systems) if project time had allowed. Support from this project is consistent with best practices highlighted by other initiatives, notably the publication of the IAPH 2021 Cybersecurity Guidelines for Ports and Port Facilities and the IMO Maritime Cyber Risk Management Guidelines.

In addition to the bottom-up approach of WeCAPS, a national cyber resilience law would be welcomed by port decision-makers. The African Union made a positive start in 2014 with the adoption of the Convention on Cyber Security and Personal Data Protection (the Malabo Convention)[71] and could be the first step towards this legislation. In addition, African countries and private terminal operators could jointly adopt best practices to ensure the security of their maritime infrastructures.

[70] (Africa's Maritime Cyber Security Progress After the Transnet Attack, 2021)

[71] (African Union Convention on Cyber Security and Personal Data Protection, 2014)

8 Conclusions

Maritime CII includes, among others, ports, ships and maritime companies. The maritime CIIs are secure if their physical assets are safe and their cyber assets are cybersecure. This study covered all aspects that are important for the security of maritime CIIs including: legal and policy, technological, standards and guidelines.

9 Recommendations

The purpose of this study is not to create a handbook of best practice, but to briefly list the issues that must be addressed to build a high-performing cyber shield. The best practices mentioned below will help port and ship operators comply with IMO's cybersecurity risk management requirements enhancing the security and trustworthiness of the international supply chains and trade.

9.1 Recommendations to Sub-Saharan African ports

As this report has demonstrated, a holistic approach to security is essential. These first recommendations look at physical security which would complement the recommendations to improve cybersecurity listed further below. The recommendations here are based on observations in several ports in Sub-Saharan Africa, where potential improvements in the security shield are possible:

1. International support to African countries to optimise their national maritime security laws applicable to the juridical administrative port zones, by assessing the actual port police and customs regulations, national ISPS and port security regulations, and other national regulations.
2. Strengthen the capacity of security personnel through various initiatives, such as:
    - Drone pilot training (against potential airborne attacks)
    - ISPS Port Facility Security Officer Training and training for security guards in cooperation with IMO
    - Security guards with trained security dogs (against drugs, chemicals, explosives)
    - Management training for security personnel in SEMS Security Management Systems
    - Expert advice on the installation of access control systems, perimeter control systems and Port Security Control Centres
    - RIB boat crew training and interception training within port areas
    - Surveillance training for boat crews to prevent pirate attacks for vessels at anchor
    - Port Police training regarding port security tasks and ISPS regulations
    - Inspection and auditor trainings for Designated Authorities and Port State Control
    - Installation of port security committees involving private and governmental actors
3. Deliver critical equipment for security personnel in the ports and for private terminal operators, allowing them to execute their tasks efficiently, such as:
    - Drones for police and security personnel
    - Rigid Inflatable Boats (RIB) for marine patrol security guards and police
    - Communication equipment for security personnel on land and in the water
    - Inspection equipment for security guards at port entries
    - Tagging systems for mobile patrol guards
    - X-ray scanners to inspect cargo for Customs
4. Accompany the navy, police, port, and maritime designated authorities in their efforts to improve standard operating procedures and emergency response planning on the water bound port areas, to enhance the security of anchored vessels, port access channels and port basins.

5. Strengthen the relationship between the different port stakeholders in the various countries through expertise-sharing seminars and technical workshops. Involving Ministries of Transport and National security, Designated Authorities, port decision makers, ports from Europe and elsewhere, IMO, USCG, European Commission, The Shipowners' Club – Protection and Indemnity (P&I) and other Insurance organisations, shipping companies and private terminal operators active in the continent.

9.2 Recommendations to African maritime stakeholders

African countries in general need to improve their cybersecurity legislation, like many other maritime bound countries in the world. Besides the port security initiatives, it is observed that several ports still face challenges in making their ports highly resilient against security and cybersecurity attacks. Therefore, additional port security initiatives are needed by aiding national legislators, port authorities, private terminal operators, national designated authorities, police, private port security companies and other stakeholders in and around ports. It is highly recommended that these ISPS initiatives are strengthened together with cybersecurity initiatives within the legal-administrative port area (on land and in the water). These initiatives would create an operational framework through capacity building, supporting the development of appropriate infrastructure and equipment, training, and coaching, and expanding international partnerships.

9.3 Senior Management Support

Senior management is becoming increasingly aware of cyber threats and risks and their potentially devastating impact on ship and port operations. The necessary ongoing investment in cybersecurity will specifically target cybersecurity personnel, security management, processes, and technologies. This requires the allocation of budget and resources and must be approved and supported by senior management. Cyber risks affect, and can be affected by, everyone in ports and on ships. Therefore, cybersecurity measures should not be the responsibility of the IT department alone.

9.4 Cybersecurity awareness training

Everyone aboard a ship or in a port should be aware of threats and how cyber incidents affect them. Therefore, they should receive cyber awareness training so that they know what they can do to ensure that the port and ship remain safe. The training should be tailored by function.

9.5 Cybersecurity procedures, guidelines, and instructions

Port and ship personnel need to know exactly what is expected of them and how to manage cybersecurity. They should receive Standard Operating Procedures (SOP) on how to manage their daily tasks as well as incident management. Cybersecurity teams should be formed, have regular meetings and have an impact on the operations.

9.6 Critical services and functions in the organisation

To know how to address cybersecurity, it is vital to know what systems exist in the port and aboard ships. An inventory should include all critical physical and cyber assets, including devices, systems, software and applications for both IT and OT.

9.7 Cybersecurity risks assessment

With the inventory in hand, a risk assessment should be conducted to identify threats, risks and vulnerabilities related to IT and OT assets that could negatively impact operations and security.

9.8 Cybersecurity management plan

In addition to existing ISPS port (facilities) security plans and ship security plans, a cybersecurity management plan should be developed, as these plans focus mainly on physical security. This plan will include measures to address identified risks based on the risk assessment, crew cybersecurity responsibilities, procedures to respond to cybersecurity threats and procedures for auditing cybersecurity activities. The plan would include both procedural and technical measures to be implemented to minimise cyber risks.

9.9 Supply chain cybersecurity

Equipment suppliers may have remote access to critical systems on board (e.g., navigation systems, engine supply systems, cargo systems, etc.) or at the port facilities (e.g., container spreaders, harbour cranes, RMG and RTG systems, etc.), and any cybersecurity incident on the supplier side may affect the ship or the specific handling equipment and systems for which they are responsible. Therefore, it is important to assess the cybersecurity of the suppliers to identify risks in their services and systems that could negatively affect the operation of the ships and ports.

9.10 Incident management, response, and recovery

Ships and ports must implement appropriate policies, procedures and controls that enable them to detect, respond to, recover from, learn from, and improve cybersecurity incidents.

9.11 Cybersecurity standards and frameworks

It is not easy to manage all aspects of cybersecurity management without using help and guidance from existing standards and guidelines. Therefore, cybersecurity management should use policies, processes and procedures on technical controls and employee awareness to manage cybersecurity in ports and aboard ships. Expert advice from maritime consultants who can help implement cybersecurity in the port and ship environment is important to avoid mistakes.

9.12 General Port cybersecurity recommendations

The cybersecurity recommendations listed below to be implemented in seaports would make a positive cybersecurity difference to port authorities and other stakeholders working in the port.

1. Cybersecurity Port legislation

Implement/adjust national legislation to become compliant with international port cybersecurity legislation, codes, and guidelines as this is the driver for trustworthy international trade.

2. Cybersecurity Assessment (CSA)

In accordance with ISPS security standards, security assessments (PSA and PFSA) are carried out for ports and port facilities. The purpose of these assessments is to identify vulnerabilities in physical structures, personnel protection systems and business processes that could lead to a security incident. The Cybersecurity Assessment is intended to build on existing ISPS security assessments where appropriate. Use existing standards (e.g., ISO270xx) and international best practices (e.g., IMO/BIMCO, ENISA, IACS) to assess, estimate and mitigate cyber and physical risks.

3. Cybersecurity Plan (CSP)

Security assessments form the basis of port (PSP) and port facility security plans (PFSP). These plans address the issues identified in the relevant assessment by establishing appropriate security measures designed to minimise the likelihood of a security breach and the consequences of potential risks. The cybersecurity plan is intended to build on the existing PSP or PFSP where appropriate. Testing a plan, preferably with tabletop exercises, is also important to ensure the plan is up-to-date and understood by all stakeholders.

A CSP has the same function as the ISPS security plan for the issues identified in the CSA, also considering the impact of the measures set out in the PSP and PFSP.

4. Cyber organisation

For cybersecurity management, it is vital to have an organisational chart in which different stakeholders are given specific roles and tasks.

- The nomination of a Ship Cyber Security Officer (CYSO), being responsible for cybersecurity of the port and port facilities who are managed by the port.
- Installation of a Port Security Committee where different stakeholders attend.
- The establishment of a Security Operations Centre (SOC).

5. Managing cybersecurity

After the cybersecurity shield is in place through the establishment of the CSA and CSP, it is important that the SOC has appropriate management and operational arrangements in place, including:

- Regular audit and review of the CSP
- Regular cyber-attack tests
- Monitoring of the evolution of the cyber shield
- Methods to provide information to third parties
- How to manage security incidents
- Regular tests of the plans and incident management through tabletop exercises

6. Capacity building training

People work with OT and IT systems and need regular training to work efficiently. Therefore, training at different levels is vital:

- Training for security personnel (operators), who use the security OT and IT systems daily.
- Training for security management (PFSO, PSO), to understand the consequences and impact on security IT and OT systems. They must be able to minimise damages,

implement immediate security countermeasures and return to the normal situation as soon as possible.

- Training for IT personnel, who are involved in the security OT systems. They must be able to install and improve the cybersecurity shield for the security personnel.

The above security recommendations are outlined in the next Table:

N°	Recommendations
1	Optimise national maritime security laws (port police and customs regulations, national ISPS and port security regulations)
3	ISPS Port Facility Security Officer Training and training for security guards in cooperation with IMO
4	Security guards with dogs/ smart gates training (against drugs, chemicals, etc)
5	Training for security personnel in SEMS Security Management Systems
6	Advice on the installation of access control systems, perimeter control systems and Port Security Control Centres
7	RIB boat crew training and interception training within port areas
8	Surveillance training for boat crews to prevent pirate attacks for vessels at anchor
9	Port Police training regarding port security tasks and ISPS regulations
10	Inspection and auditor trainings for Designated Authorities and Port State Control
11	Installation of port security committees involving private and governmental actors
12	Deliver security certified equipment for security personnel in the ports and for private terminal operators (drones, RIBS, Communication equipment, Inspection equipment, Tagging systems and X-ray scanners)
13	Accompany DA, police, navy to improve standard operating procedures and emergency response planning (on land and on the water)
14	Strengthen relationship between the different international port stakeholders.
15	Improve national port cybersecurity legislation, practices and procedures
16	Cybersecurity Assessment and cybersecurity management
17	Establish, implement, audit and continuously improve the Cybersecurity Plan
18	Nominate a Cybersecurity Officer and a cybersecurity team
19	Install a Port Security Committee
20	Collaborate/establish and operate a SOC
21	Organise a daily management group to address incidents and other daily cybersecurity tasks
22	Training for security personnel (security operators)
23	Training for security management (PFSO, PSO)
24	Training for IT personnel, who are involved in the security OT systems

9.13 Recommendations to the EU: Towards a stable EU-Africa collaboration

An EU-African collaboration in the following areas would enhance the maritime global security and the security of our supply chains:

- *Build stable collaborations* between Ministries of Maritime/Transport, Security Agencies and maritime ISACS to reach common understanding, continuous monitoring, mitigate security challenges and cross-border security incidents in the maritime ecosystem. Build strong synergies and exchange knowledge, recommendations, and best practice.
- *Maritime security awareness campaigns and training*: Build collaboration with public and private entities to develop centres for maritime security awareness raising, operational training and incident handling training targeting general maritime and shipping -specific security needs where simulation and exercise platforms would facilitate skills development.
- *Close the cyber skills gap* with hands-on risk assessments, virtual simulation of industrial attacks and incidents targeting the shipping industry, and the general maritime and international supply chain digital ecosystem. Extensively using cyber-ranges can help the shipping industry stakeholders to improve their understanding in handling complex attacks and incidents and improve preparedness and resilience in the shipping sector. This would involve realistic evidence-based experiments and "capture the flag" exercises with cybersecurity and attack teams pitted against each other. The International Association of Classification Societies (IACS) and IMO can build upon the ENISA-Cyber Europe experience and further collaborate with ENISA and CERT-EU to promote the cybersecurity training and pave the way forward to effective training in the maritime sector.
- *Cross-border support in operating maritime SOCs* that will effectively forecast and manage cyber-attacks and security incidents.
- *Harmonise maritime certification efforts*: Jointly audit and assess the security of the maritime equipment to ensure privacy, security, transparency, interoperability, accountability, liability and compliance with EU and international security legislation and guidelines. Encourage EU and African communities (military and civilian) of manufacturers, developers, and integrators to adopt the culture of sharing responsibilities for security by performing common conformance testing using international standards.
- *Benchmark* regularly by conducting comparative analysis between ports in the EU, in the Sub-Saharan African region and ports in other regions of the world, such as Southeast Asia. This would be useful to highlight successful EU-African security and cybersecurity approaches that can be replicated in other regions.

10 References

Acharya, T. (2019, July 31). *Black boxes and their intrusion*. Available at Towards Data Science: https://towardsdatascience.com/black-boxes-and-their-intrusion-620aa3c4c56b

Africa Maritime Technology Cooperation Centre launched in Mombasa. (2017, December 13). Accessed at EEAS: https://www.eeas.europa.eu/node/37286_en

African Union Convention on Cyber Security and Personal Data Protection. (2014). African Union. Accessed at https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Africa's Maritime Cyber Security Progress After the Transnet Attack. (2021, September 16). Accessed at The Maritime Executive: https://maritime-executive.com/article/africa-s-maritime-cyber-security-progress-after-transnet-attack

Alcaide, J. I., & Garcia-Llave, R. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia, 45*, 547-554. doi:10.1016/j.trpro.2020.03.058

Alderton, P. (1999). *Port Management and Operations.* LLP Professional Publishing.

Ashraf, I., Park, Y., Hur, S., Kim, S., Alroobaea, R., Bin Zikria, Y., & Nosheen, S. (2022). A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Transactions on Intelligent Transportation Systems*, 1-14. doi:10.1109/TITS.2022.3164678

Atlantic Area Units. (s.d.). Available at United States Coast Guard Atlantic Area: https://www.atlanticarea.uscg.mil/Our-Organization/Area-Units/

Burt, J. (2021, August 10). Cybersecurity Landscape and Threats to Maritime Operations. Accessed at https://www.tenntom.org/wp-content/uploads/2021/10/CISA-Jason-Burt_CISA_Cybersecurity-Port_Maritime-Security.pdf

China hackers steal data from US Navy contractor - reports. (2018, June 9). Accessed at BBC: https://www.bbc.com/news/world-us-canada-44421785

Code of Safe Practice for Cargo Stowage and Securing (CSS Code). (s.d.). Accessed at IMO: https://www.imo.org/en/OurWork/Safety/Pages/CSS-Code.aspx

Company, R. (2017, July 21). *How ports can protect themselves against cyber and physical security threats*. Accessed at Medium: https://medium.com/@ICHCA/how-ports-can-protect-themselves-against-cyber-and-physical-security-threats-b6bd10c4f7a7

Costa Concordia: What happened. (2015, February 10). Accessed at BBC: https://www.bbc.co.uk/news/world-europe-16563562

Coulibaly, S., Kassa, W., & Zeufack, A. (2022, June). *Re-engineering African trade with the European Union and United States: Success requires reform on both sides*. Accessed at World Bank Blogs: https://blogs.worldbank.org/africacan/re-engineering-african-trade-european-union-and-united-states-success-requires-reform

Darbra, R.-M., & Casal, J. (2004, February). Historical analysis of accidents in seaports. *Safety Science, 42*(2), 85-98. doi:10.1016/S0925-7535(03)00002-X

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (2016). Accessed at https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Drougkas, D. A., Sarri, A., Kyranoudi, P., & Zisi, A. (2019, November 26). *Port Cybersecurity - Good practices for cybersecurity in the maritime sector.* ENISA. Accessed at ENISA: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

ENISA Threat Landscape 2022. (2022). European Union Agency for Cybersecurity (ENISA). Accessed at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Erstad, E., Ostnes, R., & Lund, M. (2021, March). An Operational Approach to Maritime Cyber Resilience. *TransNav, 15*(1). doi:10.12716/1001.15.01.01

ESPO: The First Port of Call for European Transport Policy Makers in Brussels. (s.d.). Accessed at ESPO: https://www.espo.be/

EU-Africa: Global Gateway Investment Package. (s.d.). Accessed at European Commission: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway/eu-africa-global-gateway-investment-package_en

European Maritime Safety Agency . (s.d.). Accessed at EMSA: https://www.emsa.europa.eu/

European Union Agency for Cybersecurity (ENISA). (2020). ENISA Threat Landscape: 15 Top Threats in 2020. Accessed at https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape-2020-top-15-threats

Good Pratice Guide: Cyber Security for Ports and Port Systems. (2020). The Institution of Engineering and Technology. Accessed at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf

Greater and More Diverse Participation in Global Trade is Key to Achieving Africa's Economic Transformation, says New World Bank Book. (2022, February 10). Accessed at The World Bank: https://www.worldbank.org/en/news/press-release/2022/02/10/greater-and-more-diverse-participation-in-global-trade-is-key-to-achieving-africa-s-economic-transformation-says-new-wor

Greenberg, A. (2018, August 22). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Accessed at Wired: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Guidelines - Cyber Risk Management for Ports. (2020). European Union Agency for Cybersecurity (ENISA). Accessed at https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports

Guidelines on Maritime Cyber Risk Management. (2017). London: IMO. Accessed at https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

Gulf of Guinea Map. (2021, February 10). Institute for Security Studies. Accessed at https://issafrica.s3.amazonaws.com/site/images/2021-02-10-gulf-of-guenea-piracy-map.png

Hand, M. (2020, April 17). *MSC confirms malware attack caused website outage*. Accessed at Seatrade Maritime News: https://www.seatrade-maritime.com/containers/msc-confirms-malware-attack-caused-website-outage

Herald of Free Enterprise Ferry Disaster – 1987. (s.d.). Accessed at Devastating Disasters: https://devastatingdisasters.com/herald-of-free-enterprise-ferry-disaster-1987/

ILO: International Labour Oeganization. (s.d.). Accessed at UN: Office of the Secretary-General's Envoy on Youth: https://www.un.org/youthenvoy/2013/08/ilo-international-labour-organization/?gclid=CjwKCAiAv9ucBhBXEiwA6N8nYF5eTI5UjefYhsbZBgjQa8jYr3hWW0MocPuYj4mAk-nPawYFcgjb1hoCS3QQAvD_BwE

International Convention for the Safety of Life at Sea (SOLAS), 1974. (s.d.). Accessed at IMO: https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 197. (s.d.). Accessed at IMO: https://www.imo.org/en/OurWork/HumanElement/Pages/STCW-Convention.aspx

Inventory of Risk Management / Risk Assessment Methods and Tools . (s.d.). Accessed at European Agency for Cybersecurity (ENISA): https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory

ISO/IEC 27001 and related standards: Information security management. (s.d.). Accessed at ISO: https://www.iso.org/isoiec-27001-information-security.html

Jørgensen, R. N. (2018). *Cyber security survey shows more action is needed in the industry*. Accessed at BiMCO: https://www.bimco.org/news/priority-news/20180924-cyber-security-survey

Kalogeri, E., & Polemi, N. (2022). A taxonomy of maritime security standards. *6th NMIOTC Conference on Cyber Security in Maritime Domain.* Souda Bay: NATO.

Kioskli, K., & Polemi, N. (2020). A Socio-Technical Approach to Cyber-Risk Assessment. *International Journal of Electrical and Computer Engineering, 14*(10), 305-309. Accessed at https://publications.waset.org/10011507/a-socio-technical-approach-to-cyber-risk-assessment

Kioskli, K., & Polemi, N. (2020). Psychosocial Approach to Cyber Threat Intelligence. *International Journal of Chaotic Computing, 7*(1), 159-165. doi:10.20533/ijcc.2046.3359.2020.0021

Langewiesche, W. (2004, May). A Sea Story. *The Atlantic*. Accessed at https://www.theatlantic.com/magazine/archive/2004/05/a-sea-story/302940/

Maritime trade and Africa. (2018, October 3). Accessed at UNCTAD: https://unctad.org/press-material/maritime-trade-and-africa

Measures to Enhance Maritime Security: IAPH Cybersecurity Guidelines for Ports and Port Facilities. (2021). IMO. Accessed at https://events.iala-aism.org/content/uploads/2021/09/MSC-104-7-1-IAPH-Cybersecurity-Guidelines-for-Ports-and-Port-Facilities-IAPH.pdf

Meland, P., Bernsmed, K., Wille, E., Rødseth, Ø., & Nesheim, D. (2021, September). A Retrospective Analysis of Maritime Cyber Security Incidents. *TransNav, 15*(3). doi:10.12716/1001.15.03.04

MTCC Africa. (s.d.). Accessed at MTCC Africa: http://mtccafrica.jkuat.ac.ke/

Negreiro, M. (2022). *The NIS2 Diretive: A high common level of cybersecurity in the EU.* Accessed at https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

NIST Risk Management Framework (RMF). (s.d.). Accessed at NIST: Computer Security Resource Center: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/

Our Work. (s.d.). Accessed at IMO: https://www.imo.org/en/OurWork/Pages/Default.aspx

Polemi, N. (2017). *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains.* Elsevier. doi:9780128118191

Port of San Diego: phishing emails remain amongst greatest cyber threats. (2021, August 19). Accessed at Port Technology International: https://www.porttechnology.org/news/port-of-san-diego-phishing-emails-remain-amongst-greatest-cyber-threats/#:~:text=The%20Port%20of%20San%20Diego%20reported%20a%20ransomware,hacker%20operating%20inside%20the%20Islamic%20Republic%20of%20Iran.

Resolution A.682 (17). (1991). International Maritime Organization. Accessed at https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.682(17).pdf

Reva, D. (2020). *Maritime cyber security: Getting Africa ready.* Institute for Security Studies. Accessed at https://issafrica.s3.amazonaws.com/site/uploads/ar-29-2.pdf

Rulebook 2021. (s.d.). UKP&I. Accessed at https://www.ukpandi.com/news-and-resources/rulebook-2021/

Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports. (s.d.). Accessed at CORDIS: https://cordis.europa.eu/project/id/740477

Shapira, I. (2006, January 4). Captain Blamed in Fatal Tanker Explosion Off Va. *The Washington Post*. Accessed at https://www.washingtonpost.com/archive/local/2006/01/04/captain-blamed-in-fatal-tanker-explosion-off-va/f4a4ffc8-6cea-4893-ba6c-e9afd76eec8d/

SOLAS XI-2 and the ISPS Code. (s.d.). Accessed at IMO: https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

Standards. (s.d.). Accessed at ISO: https://www.iso.org/standards.html

Strenghtening Africa's gateways to trade. (2018). PwC. Accessed at https://www.pwc.co.za/en/assets/pdf/strengthening-africas-gateways-to-trade.pdf

The Beirut Port Explosion. (s.d.). Accessed at Forensic Architecture: https://forensic-architecture.org/investigation/beirut-port-explosion

The Guidelines on Cyber Security onboard Ships - Version 4. (2020). BIMCO. Accessed at https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

The International Safety Management (ISM) Code. (s.d.). IMO. Accessed at https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx

Threat Landscape for Supply Chain Attacks. (2021). European Union Agency for Cybersecurity (ENISA). Accessed at https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Titanic. (s.d.). Accessed at Britannica: https://www.britannica.com/topic/Titanic/Aftermath-and-investigation#ref302525

Tomter, L., & Gundersen, M. (2019, April 14). *IT-sjefen i Hydro om dataangrepet: – Man tror krisen blir stor, så blir den enda verre*. Accessed at NRK: https://www.nrk.no/norge/it-sjefen-i-hydro-om-dataangrepet_-_-man-tror-krisen-blir-stor_-sa-blir-den-enda-verre-1.14515043

WeCAPS. (s.d.). Accessed at Strengthening the security and safety of ports in West and Central Africa : https://wecaps.eu/en/

Widup, S. (2019). *2019 Verizon Data Breach Investigations Report.* Verizon. Accessed at https://www.nist.gov/system/files/documents/2019/10/16/1-2-dbir-widup.pdf

Winder, D. (2019, July). *U.S. Coast Guard Issues Alert After Ship Heading Into Port Of New York Hit By Cyberattack*. Accessed at Forbes: https://www.forbes.com/sites/daveywinder/2019/07/09/u-s-coast-guard-issues-alert-after-ship-heading-into-port-of-new-york-hit-by-cyberattack/?sh=78d82cb141aa

11 Annexes: Security Questionnaires

11.1 Annex A: Security Governance Awareness Questionnaire

Based on ISO27001[72], the following questionnaire can serve to benchmark the governance structure of a maritime enterprise to manage security risks:

Control Objective	Topic	Question	No	Yes
Security (safety and cybersecurity) policy	Information security policy	Is the personnel aware of the security policy link with his duties?		
Organisation of security	Internal organisation	Is the personnel aware of their security responsibilities?		
		Does the personnel hold the necessary authorisations?		
	External parties	Is the personnel aware of possible risks when dealing with external parties?		
		Is the personnel taking security measures when dealing with customers?		
Asset management	Responsibility for assets	Is the personnel aware of the assets is dealing with?		
		Is the personnel aware of the ownership of these assets?		
		Is the personnel aware of the usage of the assets?		
	Information classification	Is the personnel aware of the classification guidelines?		
		Is the personnel aware of the information labelling and handling?		
Human resources security	During employment	Does the personnel know his management responsibilities?		
		Has the personnel been trained in security awareness topics in safety (e.g., access control measures) and cybersecurity (e.g., phishing, social engineering, storage of data)?		
	Termination of employment	Does the personnel know that on the termination of employment they have to		

[72] From the International Organization for Standards (ISO); https://www.iso.org/isoiec-27001-information-security.html

		return its assets and the access rights are removed?		
Physical and environmental security	Secure areas	Is the personnel aware of the Physical security perimeter of the port?		
		Is the personnel aware of the Physical entry controls?		
		Is the personnel aware of the procedure securing the place of work?		
	Equipment security	Is the personnel aware of the use of the security and IT equipment within the premises?		
		Is the personnel aware of the policy on the Bring your own device?		
		Is the personnel aware of the procedures on the secure disposal or re-use of equipment?		
Communications and operations management	Operational procedures and responsibilities	Is the personnel aware of the operating procedures link with the activities?		
		Is the personnel aware of the change management process ?		
	Protection against malicious and mobile code	Is the personnel aware of controls against malicious code (i.e., handling emails)?		
		Is the personnel aware of controls against mobile code (i.e., infected mobile devices)?		
	Back-up	Is the personnel aware of the process of the information back-up?		
	Media handling	Is the personnel aware of the management of removable media?		
		Is the personnel aware of the disposal of media?		
		Is the personnel aware of the information handling procedures?		
		Is the personnel aware of the security of system documentation?		
		Is the personnel aware of the protection of the physical media in transit?		

	Exchange of information	Is the personnel aware of electronic messaging?		
	Electronic maritime services	Is the personnel aware of the procedure on the on-line transactions and the use of publicly available information?		
	Monitoring	Is the personnel aware of the policy regarding the logs?		
Access control	Business requirement for access control	Is the personnel aware of the access control policy?		
	User access management	Is the personnel aware of the procedure of the user registration?		
		Is the personnel aware of the user password policy/management?		
		Is the personnel aware of the procedure of the user access rights?		
	User responsibilities	Is the personnel aware of the password use?		
		Is the personnel aware of the procedure of unattended user equipment?		
		Is the personnel aware of the clear desk and clear screen policy?		
	Network access control	Is the personnel aware of the policy on the use of network services?		
	Operating system access control	Is the personnel aware of the secure log-on procedures?		
		Is the personnel aware of the use of system utilities?		
	Application and information access control	Is the personnel aware of the information access restrictions?		
		Is the personnel aware of the protection of sensitive system isolation?		
	Mobile computing and teleworking	Is the personnel aware of the apply policy on the use of mobile computing and communications?		
		Is the personnel aware of the policy on the use of port/ship technologies and teleworking systems?		

Information systems acquisition, development and maintenance	Cryptographic controls	Is the personnel aware of the policy on use of crypto keys and related equipment?		
Information security incident management	Reporting information security events and weaknesses	Is the personnel aware of the procedures reporting information security events?		
		Is the personnel aware of the procedures reporting security weaknesses?		
Business continuity management	Business continuity management	Is the personnel aware of the business continuity plan and the disaster recovery plan link with the duties?		

11.2 Annex B: Security Practices Questionnaire

The following questionnaire can be distributed to the ports in order to capture the maturity of their cybersecurity practices. It can also be distributed to the maritime companies and ship owners to report and assess the security practices implemented and followed:

Questionnaire for ports and maritime operators on security

Information (optional)

Company	xxxxxx
Name	xxxxx
Position	xxxxx
Number of employees	xxxxx
Business Activity	xxxx
url	xxxxx
e-mail	xxxxxx

Date

Dear Maritime stakeholder,

The objective of this questionnaire is to understand the security awareness level of the maritime Critical infrastructure (CI) in terms of threats and vulnerability of all layers of the CI, i.e., (a) physical infrastructure, (b) telco infrastructure equipment (c) software (d) services and applications (e) data (f) users (external/internal persons and things). In addition, an overview of the services and users vis-à-vis vulnerability will be sought.
The questionnaire intends to identify whether:

- Maritime operators have put in place a security plan (port security plan and ICT security policy), to which extent it is applied and which objectives it has;
- Maritime employees and users are aware of the security issues related with their daily activities;
- Information security awareness training is offered as well as its effectiveness;
- Interrelationships between Competent Authorities and the maritime CI (e.g., ports) exist and for which reasons.

For the purposes of this survey, only the maritime CI under their capacity as operators are considered (i.e., ports that are simultaneously landlords and operators OR terminal operators). Although the survey addresses ports, it applies to any maritime CI.

The responses will be considered confidential and only aggregate figures will be reported.

For more information, you may contact:

xxxxxx

Port Security Plan

1. Does the Port offer a well-defined security management plan ;

□ Yes – go to questions 1a

□ No – go to question 2

1a. Which model for security management do you adopt? [Choose only one]

□ In house – e.g., from a specific department or person(s) from the Port (e.g., PFSO)

□ Outsource – e.g., other company or organisation or external expert(s)

□ Other

1b. Which better describes your perception of security: [Choose only one]

□ Does not concern/influence your business activities

□ It is not your first priority, but you plan to consider it in the future

□ You understand its necessity, but it is too expensive to consider it

1c. Which Security Schemes does your security plan cover? [Choose as many as appropriate]

□ ISPS

□ ISO 9001, ISO 14001 (Cruise Port Services)

□ ISO 27001

□ ISO 27002

□ ISO 28000

□ Other: PERS (Port Environmental Review System, for the whole port area)

□ Other (Which:_______________________________________)

1d. Does your Security Scheme identify and analyse the following in depth?

		Our Security Plan covers it, and…	
Activities	Our Security plan doesn't cover this.	stakeholders present valid documents, but we don't analyse them.	we keep an active database of them and have specific detailed processes for analyses
Ship security plans	□	□	□
Ship security officers	□	□	□
Company security officers	□	□	□

Activities	Our Security plan doesn't cover this.	Our Security Plan covers it, and…	
		stakeholders present valid documents, but we don't analyse them.	we keep an active database of them and have specific detailed processes for analyses
On Board equipment	□	□	□
Corresponding Port facility security plans	□	□	□
Port facility security officers	□	□	□
Certain security equipment	□	□	□
Certain security features	□	□	□
Monitoring the activities of people and cargo	□	□	□
Secure communications	□	□	□
Secure access in port sectors (monitoring, control)	□	□	□
Cyber Port Policy	□	□	□
Other (please specify)	□	□	□
Don't know	□		

2. Did you consider security issues in the following activities of the Port in the past 12 months? If yes, were your reactions proactive or reactive?

Activities	Security issues were not considered	Yes, security issues were considered	
		Nature of action	
		proactive	reactive
Improvements in your services/products/business / supply chains	□	□	□
Industry compliance	□	□	□
Improvements in the operation of your IT systems	□	□	□
Improvements in the operation of your Port Facilities entry/exit/perimeter systems	□	□	□

Activities	Security issues were not considered	Yes, security issues were considered	
		Nature of action	
		proactive	reactive
Improvements in your business profile and confidence level of your users and services	□	□	□
Compliance with EU legislation influencing your international operation and supply chains	□	□	□
Privacy and Data Protection	□	□	□
Safety of personnel and users	□	□	□
Secure access in port sectors	□	□	□
Don't know	□		

3. Select three (3) main categories of regulations/legislation that influence your operation and security measures in the past/next 12 months. Indicate if you consider any security projects in your selections.

Types of Regulations	In the last 12 months	In the next 12 months	Security Projects in Progress/under consideration
Internal Audit:			
ISPS	□	□	□
ISM	□	□	□
ISO Families of Standards	□	□	□
OHSAS 18000 Families	□	□	□
Sarbanes-Oxley	□	□	□
Regulation (EC) 725/2004	□	□	□
SOLAS/MARPLE standards			
Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.	□	□	□
Data Protection (e.g., GDPR,NIS, NISII, ISO 27000/27001/27002/27005, ISO15048, ISO18045)	□	□	□

Types of Regulations	In the last 12 months	In the next 12 months	Security Projects in Progress/under consideration
Sectored Regulations (e.g., PCI Data Security Standard)	□	□	□
Customs and Financial Authorities Regulations	□	□	□
Other (Problems with the Customs ________________________________)	□	□	□
Other (No problems with Financial Authorities ________________________________)	□	□	□
Other (please define________________________________)	□	□	□

4. Select five (5) cybersecurity issues in terms of importance (1 = lowest importance, 5 = highest importance) for your enterprise. Do you have a plan for addressing these security issues?

Cybersecurity security Issues	Important security issue	Plan of Response		
		Now	Next 12 months	No plan
Secure Data dissemination (to competent authorities, supply chain providers, maritime companies etc.)	□	□	□	□
Secure storage of data	□	□	□	□
Access (Physical) to/from Port Facilities	□	□	□	□
Secure Port services (containers management, LNG, supply chain services)	□	□	□	□
Radio Frequency Identifiers (RFID)	□	□	□	□
Mobile Devices (e.g., PDA, smart phones)	□	□	□	□
Automated Border Control (ABCs) systems	□	□	□	□
Mobile Storage (e.g., USB flash drive, portable drives)	□	□	□	□
Voice-over-IP telephony	□	□	□	□
Web Services	□	□	□	□
Wireless Networks	□	□	□	□
Secure Satellite Communication	□	□	□	□
New operation systems	□	□	□	□
Cryptography of e-mails	□	□	□	□
Cryptography of hard drive	□	□	□	□

Cybersecurity security Issues	Important security issue	Plan of Response		
		Now	Next 12 months	No plan
	□	□	□	□

Security Practices

5. How do you check the security level of your enterprise? [Choose more than one if necessary]

□ Internal Audit (from Security Department)
□ External Audit
□ Internal Assessment from personnel
□ Other
□ We do not have such procedures

6. Select five (5) main security activities in terms of importance (1 = lowest importance, 5 = highest importance) for your Port. Independently select five (5) main security activities in terms of required implementation time (1 = short time consuming , 5 = high time consuming):

	Importance	**Implementation Time**
Compliance with ISP	□	□
Compliance with ISO27001, 27005	□	□
Business continuity management	□	□
Risk and security management	□	□
Pursue, development, integration of IT systems	□	□
Access –Control Management	□	□
Communications and Operations Management	□	□
Physical Security	□	□
Protection of employees (safety)	□	□

	Importance	**Implementation Time**
Updates of services and products	□	□
Security Management	□	□
(Cyber) Security Policy	□	□
Privacy- Data Protection	□	□
Accountability	□	□
Disaster recovery Plan	□	□

7. How do you approach / solve the following security issues in your Port;

Security Issues:	No considerati on	Best Practices	Own Methods
Cybersecurity Incidents- Attacks	□	□	□
Business Continuity	□	□	□
Business Resilience	□	□	□
Cyber Risk management	□	□	□
Physical Risk management	□	□	□
Privacy and Data Protection	□	□	□
Security Mechanisms in offered e/m- port services	□	□	□

8. When you collaborate with other enterprises (e.g., outsourcing, external contractors, third parties), which of the following do you consider necessary with respect to security?

□ Your collaborators have and follow an auditable security policy

□ Your collaborators are required to use/respect your own security policy and security concerns

□ Your collaborators are ISO 27001 compliant

□ None of the above

□ Other

9. Have you ever performed a physical risk assessment?

□ Yes
□ No

10. How often do you report on the physical security risks and incidents and to whom?

	Frequency				
	Daily	Monthly	Trimester	Semester	Never
Port Facility Security Officer	□	□	□	□	□
Security company (external)	□	□	□	□	□
Police	□	□	□	□	□
Customs	□	□	□	□	□
Competent Authorities (Which:_____________)	□	□	□	□	□
Insurance Companies	□	□	□	□	□
Banks and Financial Institutions	□	□	□	□	□
Contractors and Stakeholders	□	□	□	□	□
Chamber of Commerce (or similar organisation)	□	□	□	□	□
National Certification Authority	□	□	□	□	□
Other (Which___________________________)	□	□	□	□	□
Other (Which___________________________)	□	□	□	□	□
Other (Which___________________________)	□	□	□	□	□

11. Have you ever performed a cyber risk assessment?

□ Yes
□ No

12. How often do you report on the cybersecurity risks and incidents and to whom?

	Frequency				
	Daily	Monthly	Trimester	Semester	Never
Port Cyber Security Officer	□	□	□	□	□
Security company (external)	□	□	□	□	□
Public Authorities (e.g., Police	□	□	□	□	□
Maritime Company	□	□	□	□	□
Competent Authorities (e.g., CERT, CSIRTS, ISAC, Ministry)	□	□	□	□	□
Insurance Companies	□	□	□	□	□
Banks and Financial Institutions	□	□	□	□	□
Contractors and Stakeholders	□	□	□	□	□
IMO, EMSA (or similar maritime organisation)	□	□	□	□	□
National Certification Authority	□	□	□	□	□
Other (Which______________________________)	□	□	□	□	□
Other (Which______________________________)	□	□	□	□	□
Other (Which______________________________)	□	□	□	□	□

13. How do you get informed about security issues? Which organisation would be most appropriate to get training on security? Which topics would you be most interested in? (You may make several choices)

Organisations	Security Technologies/Implementation	Security Policies	Risk Assessment	Privacy-Data Protection
Security Consultants (Private Companies)	□	□	□	□
University	□	□	□	□
National Body	□	□	□	□
Internet	□	□	□	□
Governmental Body	□	□	□	□

Organisations	Security Technologies/Implementation	Security Policies	Risk Assessment	Privacy-Data Protection
Chambers of Commerce	□	□	□	□
Industry Associations or professional bodies (e.g., IMO, EMSA, ENISA, NIST)	□	□	□	□
Press, scientific publications	□	□	□	□

14. Which security standards are you aware of?

ISO 9001	□
ISPS	□
ISM	□
SIRE / ATB Inspections	□
ISA/IEC-62443	□
US Barge and Inland ATB Inspection Request	□
EBIS Inspection	□
ISO/IEC 2700x	□
ISO 20858	□
ISO 15408, ISO18045	□
Information Security Forum	□
CobIT	□
Information Technology Infrastructure Library (ITIL)	□
Capability Maturity Model Integration (CMMI)	□
SEISMED	□
None of the above	□
Other (Which__________________________________ __)	□
Other (Which__________________________________ __)	□

Add more if necessary

15. What is the status of your Port with respect to the following security activities;

Activity	In place/ In progress	In place in the next 12 months	Not planned
Physical access using smart cards	□	□	□
Physical access using paper-based ID cards	□	□	□
Physical Access using Automated Border Control (ABCs) Systems	□	□	□
Use of different authentication technologies for physical access (e.g., proximity cards, smart cards, biometrics)	□	□	□
Use of Intrusion detections systems	□	□	□
Up-to-date anti-virus and anti-spam filters	□	□	□
Use of firewalls	□	□	□
Inspections (out of schedule) on ships	□	□	□