PORT CYBERSECURITY

Good practices for cybersecurity in the maritime sector

NOVEMBER 2019
ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe’s citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe’s critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT
For contacting the authors please use team@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS
Dr. Athanasios Drougkas, Anna Sarri, Pinelopi Kyranoudi, Antigone Zisi

ACKNOWLEDGEMENTS
For providing valuable information that helped shape the report (in alphabetical order):
Peter Alkema, Strategic policy advisor and project manager, Port of Amsterdam
Sylvie Andraud, Maritime Sector Coordinator, The National Cybersecurity Agency of France (ANSSI)
Jérôme Besancenot, Head of I.T. Department, HAROPA Port of Le Havre
Rafael Company, Director of Innovation EU, Valenciaport Foundation
Ivano Di Santo, CIO, Trieste Port Authority
Conor Farrell, IT Manager, Dublin Port Company
Yannick Herrebaut, Cyber Resilience Manager, Port of Antwerp
Tanguy Jacob, CIO, Nantes Saint-Nazaire Port
Indrek Korela, Information Systems Security Manager, Port of Tallinn
Ilias Manos, IT Security Officer, Piraeus Port Authority S.A.
Jan Schirrmacher, Port Cyber Security Officer, Bremenports
Ward Veltman, Cyber Security & Risk Officer, Port of Rotterdam
Belle Webster, Program manager Cybersecurity, Port of Amsterdam

LEGAL NOTICE
Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.
COPYRIGHT NOTICE
© European Union Agency for Cybersecurity (ENISA), 2019
Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.
# TABLE OF CONTENTS

1. INTRODUCTION  
   1.1 STUDY OBJECTIVES  
   1.2 STUDY SCOPE  
   1.3 METHODOLOGICAL APPROACH  

2. THE EU PORT LANDSCAPE  
   2.1 EU AND INTERNATIONAL POLICY AND REGULATORY CONTEXT  
      2.1.1 International context  
      2.1.2 European context  
   2.2 PORT INFRASTRUCTURE AND SERVICES  
   2.3 OVERVIEW OF KEY STAKEHOLDERS  
   2.4 HIGH-LEVEL REFERENCE MODEL  
      2.4.1 Description of the systems  
      2.4.2 Description of data flows  

3. PORT ASSET TAXONOMY  
   3.1 ASSET TAXONOMY OVERVIEW  
   3.2 DESCRIPTION OF PORT ASSETS  

4. CYBERSECURITY THREATS AND CHALLENGES  
   4.1 THREAT TAXONOMY  
   4.2 CYBERSECURITY CHALLENGES  
   4.3 DESCRIPTION OF KEY CYBERATTACK SCENARIOS  

5. SECURITY MEASURES  
   5.1 SECURITY MEASURES CATEGORISATION  
   5.2 POLICIES  
      5.2.1 Security policy and organisation  
      5.2.2 Risk and Threats Management  
      5.2.3 Security and privacy by design
5.2.4 Asset inventory and management 41
5.2.5 Cyber resilience (Business continuity and crisis management) 41

5.3 ORGANISATIONAL PRACTICES 41
5.3.1 Endpoints protection and lifecycle management 41
5.3.2 Vulnerabilities management 42
5.3.3 Human Resource Security 42
5.3.4 Supply chain management 42
5.3.5 Detection and Incident response 42
5.3.6 Control and auditing 43
5.3.7 IT and OT physical protection 43

5.4 TECHNICAL MEASURES 43
5.4.1 Network security 43
5.4.2 Access control 44
5.4.3 Administration and Configuration Management 44
5.4.4 Threat management 44
5.4.5 Cloud security 45
5.4.6 Machine-to-machine security 45
5.4.7 Data protection 45
5.4.8 Update management 45
5.4.9 Detection and monitoring 45
5.4.10 Industrial control systems security 46
5.4.11 Backup and restore 46

6. CONCLUSIONS 47

7. BIBLIOGRAPHY/REFERENCES 48

A ANNEX: OVERVIEW OF EU PORT SECTOR 54
B ANNEX: DIGITAL TRANSFORMATION IN PORTS 56
C ANNEX: CATEGORIES OF PORT STAKEHOLDERS 58
FIGURES AND TABLES

TABLES
Table 1: Detailed port services 16
Table 2: Description of port’s assets 22
Table 3: Possible impacts for ports 26
Table 4: Threat description 28
Table 5: Key statistics about ports role in the European Union 54
Table 6: Ranking of the biggest European ports 55
Table 7: Example of stakes leading to digital transformation for ports 56
Table 8: Detailed innovations that ports set up linked with “Smart Port” concept 57
Table 9: Categories of port stakeholders 58

FIGURES
Figure 1: Methodology adopted for the study 11
Figure 2: Port services and infrastructure 16
Figure 3: Overview of port stakeholders 17
Figure 4: High-level reference model of the port systems 18
Figure 5: Asset taxonomy 21
Figure 6: Threat taxonomy 27
Figure 7: Compromising of critical data to steal high value cargo or allow illegal trafficking scenario 32
Figure 8: Propagation of ransomware leading to a total shutdown of port operations scenario 34
Figure 9: Compromise of Port Community System for manipulation or theft of data scenario 35
Figure 10: Compromise of OT systems creating a major accident in port areas scenario 37
GLOSSARY

AIS: Automatic Identification System
API: Application Programming Interface
CCS: Cargo Community System
CCTV: Closed-Circuit TeleVision
CIIP: Critical Information Infrastructure Protection
CIO: Chief Information Officer
CISO: Chief Information Security Officer
CMS: Content Management System
CSIRT: Computer Security Incident Response Team
DCS: Distributed Control System
EC: European Commission
ECDIS: Electronic Charts Display Information System
EDE: Electronic Data Exchange
EFCA: European Fisheries Control Agency
EMSA: European Maritime Safety Agency
EMSW: European Maritime Single Window
ERP: Enterprise Resource Planning
EU: European Union
EUMSS: European Maritime Security Strategy
EUROPOL: European Police Officer
FAL Convention: Convention on Facilitation of International Maritime Traffic
FIMS: Fisheries Information Management System
FRONTEX: European Border and Coast Guard Agency
GDPR: General Data Protection Regulation
GPS: Global Positioning System
HMI: Human-Machine Interface
HR: Human Resources
IAM: Identity and Access Management
ICS: Industrial Control System
ICT: Information and Communication Technology
IEC: Industrial Electronic Controls
IMB: International Maritime Bureau
IMO: International Maritime Organisation
IOC: Indicator of Compromise
IoT: Internet of Things
ISM Code: International Safety Management Code
ISO: International Organization for Standardization
ISSP: Information System Security Policy
IT: Information Technology
LAN: Local Area Network
MBCO: Minimum Business Continuity Objective
MDM: Mobile Device Management
MES: Manufacturing Execution System
MFA: Multi-Factor Authentication
MS: Member State
MTO: Maximum Tolerable Outage
NIST: National Institute of Standards and Technology
OT: Operational Technology
PAM: Privilege Account Management
PCS: Port Community System
PFSA: Port Facility Security Assessment
PFSP: Port Facility Security Plan
PKI: Public Key Infrastructure
PLC: Programmable Logic Controller
PMIS: Port Management Information System
RFID: Radio Frequency Identification
RoRo: Roll-on/Roll-Off
RPO: Recovery Point Objective
RTO: Recovery Time Objective
RTU: Remote Terminal Unit
SCADA: Supervisory Control And Data Acquisition
SIEM: Security Information and Event Management
SIS: Safety Instrumented System
SOC: Security Operation Center
SOLAS Convention: Convention on Safety of Life at Sea
SQL: Structured Query Language
SSN: SafeSeaNet
TETRA: Terrestrial Trunked Radio
TOS: Terminal Operating System
USB: Universal Serial Bus
VAT: Value Added Tax
VHF: Very High Frequency
VIS: Visa Information System
VLAN: Virtual LAN
VPN: Virtual Private Network
VTMIS: Vessel Traffic Management Information System
VTS: Vessel Traffic Service
WCO: World Customs Organization
EXECUTIVE SUMMARY

Maritime transport is a crucial activity for the European Union economy. It enables import and exports of goods, supply in energy, trade within the European Union and transport of passengers and vehicles. This activity relies on more than 1 2001 seaports within the European Union, each with different organisation, interests, challenges and activities.

The global digitalization trend and recent policies and regulations require ports to face new challenges with regards to information and communication technology (ICT). Ports tend to rely more on technologies to be more competitive, comply with some standards and policies and optimize operations. This brings new stakes and challenges in the area of cybersecurity, both in the Information Technologies (IT) and Operation Technologies (OT) worlds.

This report identifies those challenges, in relation to critical operations, stakeholder’s ecosystem and assets identification. It then lists the main threats posing risks to the port ecosystem and describes key cyberattack scenarios that could impact them.

This approach allowed the identification of security measures that ports shall put in place to better protect themselves from cyberattack. The main measures identified are described below and intend to serve as good practices for people responsible for cybersecurity implementation in Port Authorities and Terminal Operators (e.g. CISOs, CIOs etc.):

- Define a clear governance around cybersecurity at port level, involving all stakeholders involved in port operations. Indeed, many companies are involved in port operation (port operators, Port Authority, pilotage company, shipping companies, etc.), it is crucial to ensure they are all involved in cybersecurity matters and aware about how they participate to the global port operation security.
- Raise awareness of cybersecurity matters at port level and infuse a cybersecurity culture. Indeed, the maritime sector is historically very aware of safety and security matters, but it seems cybersecurity is not fully integrated yet in stakeholders’ minds. This measure shall be combined with training, to ensure proper understanding of cybersecurity matters and ability to enforce it in daily operations.
- Enforce the technical cybersecurity basics, like network segregation, updates management, password hardening, segregation of rights, etc. In the context of OT, with legacy systems that usually cannot be updated, network segregation and password protection are key to ensure a correct level of cybersecurity.
- Consider security by design in applications, especially as ports use many systems, some of which are opened to third parties for data exchange. Any vulnerability on those systems can be a gate to compromise the port systems.
- Enforce detection and response capabilities at port level to react as fast as possible to any cyberattack before it impacts port operation, safety or security. Ports can rely on simple detection measures such as alerts when a specific action is done (authentication attempt on a very critical asset for example) or search for Indicators of Compromise (IOC), or on more comprehensive, using machine learning to correlate information and identify compromising patterns. Such initiatives have already started to rise within ports ecosystem2.

---

1 See https://www.globaltrademag.com/european-ports
2 See https://www.sauronproject.eu/
1. INTRODUCTION

The European Union has identified ports as critical infrastructure and defined the ports as “any specified area of land and water, with boundaries defined by the Member State in which the port is situated, containing works and equipment designed to facilitate commercial maritime transport operations” in Directive 2005/65/EC.

Ports play a crucial role at different levels for many sectors and have been the successful pioneers in Europe for interconnecting the different types of transport. As a main vehicle for European imports and exports (food, commodities, etc.) with the rest of the world, ports enable also trade and contacts between all European nations. Moreover, ports are important nodes for passengers and vehicles transportation (inter and extra-EU) and play a key role in European fishing activity.

For a number of years, ports have been undergoing a digital transformation in order to meet emerging challenges, optimise existing processes and introduce new capabilities, such as automation and real-time monitoring of operations. This digitalisation has been centred on the interconnectivity of Information Technology (IT) and Operation Technology (OT) assets and the introduction of new technological enablers, such as cloud computing, big data and Internet of Things (IoT).

This digital transformation has also led to a change in the sector’s cyber risk profile, as evident by the proliferation of cybersecurity incidents in ports over the past few years, such as the cyberattack in Antwerp port, the NotPetya Ransomware incident and its impact on Maersk and the wave of ransomware attacks in Port of Barcelona and San Diego. Indeed, this transition to the future and to concepts, such as Smart Ports, brings along cybersecurity challenges that need to be met in order for future ports to fully unlock the potential of new technologies.

1.1 STUDY OBJECTIVES

In November 2011, ENISA published the first EU report ever on cyber security challenges in the Maritime Sector. This analysis highlighted key insights, as well as existing initiatives, as a baseline for cyber security of maritime ecosystem. This new ENISA study aims at addressing the cybersecurity challenges related to the evolution of maritime port systems and services.

---

3 See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A3A32005L0060
4 See Port Digitalization with Open Data: Challenges, Opportunities, and Integrations: https://www.researchgate.net/publication/321853773_Digital_transformation_in_maritime_ports_analysis_and_a_game_theoretic_framework
5 See https://www.researchgate.net/publication/261343481_Intelligent_ports_based_on_Internet_of_Things
6 See https://www.forbes.com/sites/stevebanker/2016/04/01/the-hamburg-port-authoritys-impressive-iot-project/
9 See https://www.big-data-value.eu/pilot/transforming-transport-ports-valencia/
10 See https://www.i-scoop.eu/blockchain-smart-port-project-case-container-release-port-antwerp
11 See https://www.bbc.com/world-europe-24539417
The main objectives of the study are to build a baseline of good practices to ensure cybersecurity of port systems and services, while mapping the relevant cybersecurity challenges and threats and highlighting some attack scenarios. The study aims at being a reference point to promote collaboration on maritime port ecosystem across the European Union and raise awareness of the relevant threats. An additional important element of the study is to map port services and systems through a high-level reference model to set the scope of the work to be done and serve as a basis for future developments.

### 1.2 STUDY SCOPE

This study outlines good practices for cybersecurity in the maritime port ecosystem, both concerning IT systems and OT systems. The port ecosystem includes all the stakeholders involved in the port operations: the managing bodies of the port (Port Authorities, terminal and facility operators), national authorities (customs, police, cities, etc.), transport companies (shipping companies, railway companies, etc.) and all the service providers essential to port operations (oil companies, energy companies, etc.).

The primary target audience of this study are people in charge of IT and OT security within the port ecosystem: employees of Port Authorities and terminal operators or any other person in charge of applying these practices. The study can also be useful for secondary stakeholders in the port ecosystem: port ecosystem associations and especially members in charge of IT and OT security matters, persons in charge of IT and OT in companies interacting with ports, especially shipping companies, etc.

### 1.3 METHODOLOGICAL APPROACH

**Figure 1: Methodology adopted for the study**

**Task 1 - Definition of the project scope and identification of experts**: the first step consisted of establishing the scope of the project and selecting subject matter experts whose input and insights were considered for the development of the report. Experts mainly include port stakeholders in charge of cybersecurity as well as some national authorities.

**Task 2 - Desktop research**: during this step, extensive search for relevant documents in the context of the project was conducted. The identified sources served as a reference to develop good practices and other parts of the report.

**Task 3 - Questionnaire and series of interviews with selected subject matter experts**: a questionnaire addressing port cybersecurity topics was developed and filled in by 14 stakeholders of the port ecosystem (from 13 European Port Authorities – either cybersecurity, security, safety or IT and OT managers – and from one national cybersecurity agency, representing 11 different Member States) and used to conduct interviews with 13 of them.

**Task 4 - Analysis of collected material and report development**: the input collected from desktop research and collaboration with stakeholders were thoroughly analysed. Based on this analysis, the first draft of this report was developed.

**Task 5 - Review and validation**: The report was validated with ENISA’s subject matter experts through sharing of the draft report and through obtaining comments and feedback.
2. THE EU PORT LANDSCAPE

2.1 EU AND INTERNATIONAL POLICY AND REGULATORY CONTEXT

2.1.1 International context
At international level, the ISPS - International Ships and Port Facilities Security Code\(^{15}\), was added to the Safety of Life at Sea (SOLAS)\(^ {16}\) Convention in 2002 to recognise the role of port facilities in maritime security and define mandatory requirements and recommendations that ships and port facilities must follow. This chapter has been defined to address ports security, but requirements can be related also to ports cybersecurity to some extent (access control and authentication requirements).

The ISPS Code requires ports to design a Port Facility Security Assessment (PFSA) to identify major assets, possible threats and countermeasures and a Port Facility Security Plan (PFSP) to identify, for each of the different security levels the procedures to be followed, the measures to be put in place and the actions to be undertaken. The PFSA must address within a port facility, the following aspects: physical security, structural integrity, personnel protection systems, procedural policies, radio and telecommunication systems, including computer systems and networks and relevant transportation infrastructure. The PFSP must address access to the port facility, restricted areas within the port facility, handling of cargo, delivery of ship’s stores and monitoring the security of the port facility.

SOLAS and FAL\(^{17}\) (Facilitation of International Maritime Traffic) conventions define nine standardized forms to be used to exchange information within the maritime ecosystem, especially between port and third parties. Electronic exchange of required information is mandatory since April 9th, 2019, especially using “Single Window” systems offset up by public authorities\(^ {18}\). This standardisation of data exchanges has a strong impact on port IT ecosystems and poses new IT security challenges.

Cybersecurity for the maritime ecosystem, in particular for ships, has been only directly addressed at International level since 2017 through guidelines and recommendations to the global maritime ecosystem.

IMO Facilitation Committee (FAL) and the Maritime Security Committee (MSC) defined IMO Guidelines on maritime cyber risk management in MSC-FAL.1/Circ.3\(^{19}\). Both recognized the urgent need to raise awareness on cyber risk threats and vulnerabilities and to provide high-level recommendations on maritime cyber risk management from current and emerging cyber threats and vulnerabilities, including main areas that support effective cyber risk management (identify, protect, detect, respond and recover).

\(^{15}\) See IMO Conventions: http://www.imo.org/en/about/conventions/listofconventions/pages/default.aspx
\(^{16}\) See IMO Conventions: http://www.imo.org/en/about/conventions/listofconventions/pages/default.aspx
These guidelines make the distinction between IT systems (use of data as information) and OT systems (use of data to control or monitor physical processes). They recognize that all organizations in the shipping industry are different and shall refer to Member Governments' and Flag Administrations' requirements and relevant international or industry standards and best practices (e.g. NIST Framework\(^{20}\), ISO/IEC 27001\(^{21}\)) in order to address the most relevant security measures.

### 2.1.2 European context

Some EU regulation impacted the maritime ecosystem and directly or indirectly ports with regards to safety, security and data exchange:

- **Some chapters of the SOLAS Convention** were transposed in the European Union through several regulations; *Regulation (EC) 725/2004*\(^{22}\) focuses on enhancing ship and port facility security and on the implementation of the International Ship and Port Facility Security (ISPS) Code while *Directive 2005/65/EC*\(^{23}\) on enhancing port security. *Regulation (EC) 336/2006*\(^{24}\) focuses on the implementation of the International Safety Management Code (ISM)\(^{25}\) within maritime sector in the European Union, though it should be mentioned that the ISM code is not applicable to ports; and
- **Directive 2010/65/EU**\(^{26}\) requires that ports of the Member States accept standardised forms (FAL forms) in order to ease traffic. This directive also introduces SafeSeaNet systems\(^{27}\) established at national and European Union level to facilitate secure data exchange between Member States’ maritime authorities and other authorities’ systems (e.g. customs systems).

More concretely, Regulation (EC) No 725/2004 and Directive 2005/65/EC are the legal frameworks which support risk assessments and security plans for ports and port facilities: the Member States must design a PFSA and the Port Authorities must design their PFSP to be approved, prior to their implementation, by the Member States which are responsible for ensuring that the implementation of PFSPs is monitored.

In 2014, the *European Maritime Security Strategy (EUMSS)*\(^{28}\) was defined (and revised in 2018)\(^{29}\) as a shared and comprehensive tool to identify, prevent and respond to any challenge that affects the security of European people, activities and assets in the maritime ecosystem, including ports. This strategy identifies the maritime security risks and threats which are “terrorism and other intentional unlawful acts at sea and in ports against ships, cargo, crew and passengers, ports and port facilities and critical maritime and energy infrastructure, including cyber-attacks”. The revision of the EUMSS, as adopted by the General Affairs Council on 26 June 2018, aims at a more focused reporting process to enhance awareness and better follow-up to the strategy.

In 2016, the *Regulation (EU) 2016/679*, called the *General Data Protection Regulation (GDPR)*\(^{30}\), on the protection of natural persons regarding the processing of personal data and

\(^{20}\) See [https://www.nist.gov/cyberframework](https://www.nist.gov/cyberframework)

\(^{21}\) See [https://www.iso.org/isoiec-27001-information-security.html](https://www.iso.org/isoiec-27001-information-security.html)

\(^{22}\) See more about European Directives and Regulations: [https://eur-lex.europa.eu/homepage.html](https://eur-lex.europa.eu/homepage.html)


\(^{27}\) See more about SafeSeaNet systems: [http://www.emsa.europa.eu/ssn-main.html](http://www.emsa.europa.eu/ssn-main.html)


on the free movement of such data, defined requirements for the protection of personal data, applied for all sectors including the maritime sector.

The Directive 2016/1148 (NIS Directive)\(^{31}\) is an EU-wide cybersecurity legislation harmonizing national cybersecurity capabilities, cross-border collaboration and the supervision of critical sectors across the EU. The recitals number 10 and 11 are specific to the maritime sector: “security requirements for companies, ships, port facilities, ports and vessel traffic services under Union legal acts cover all operations, including radio and telecommunication systems, computer systems and networks” and “when identifying operators of essential services “in the water transport sector, Member States should take into account existing and future international codes and guidelines developed in particular by the International Maritime Organisation, with a view to providing individual maritime operators with a coherent approach”.

Operators of essential services identified in the water transport ecosystem are the following:

- **Inland, sea and coastal passenger and freight water transport companies**, as defined for maritime transport in Appendix I to Regulation (EC) 725/2004\(^{32}\) not including the individual vessels operated by those companies;
- **Managing bodies of ports** (defined as “any specified area of land and water, with boundaries defined by the Member State in which the port is situated, containing works and equipment designed to facilitate commercial maritime transport operations” in the Directive 2005/65/EC\(^{33}\) including their port facilities (defined as “a location where the ship/port interface takes place; this includes areas such as anchorages, awaiting berths and approaches from seaward, as appropriate” in the Regulation (EC) No 725/2004\(^{34}\)) and entities operating works and equipment contained within ports; and
- **Operators of vessel traffic services** (defined as “service designed to improve the safety and efficiency of vessel traffic and to protect the environment, which has the capability to interact with the traffic and to respond to traffic situations developing in the VTS area” in the Directive 2002/59/EC\(^{35}\)).

Finally, in 2019, the EU Cybersecurity Act\(^{36}\) strengthens the position of ENISA within cybersecurity matters for EU Member states and defines an EU-wide cybersecurity certification framework for ICT products, services and processes. This framework will provide a comprehensive set of rules, technical requirements, standards and procedures in order to attest that ICT products and services can be trusted based on EU requirements.

In addition to International and European regulatory and policy initiatives, several Member States have also developed their own initiatives to improve cyber risk management in general or specifically in the maritime sector such as national cybersecurity strategies, good practices or recommendations, for example the French CIIP law\(^{37}\), UK’s cyber security code of practice for ports\(^{38}\), German “IT-Grundschutz”\(^{39}\), etc.

---

\(^{34}\) See https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32004R0725
\(^{36}\) See https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
\(^{39}\) See https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutz_node.html
2.2 PORT INFRASTRUCTURE AND SERVICES

The port infrastructure and services exhibit a high degree of diversity from one port to another and from one Member State to another: over the years, the ports have adapted their infrastructure and services to the local geographic and territorial specificities, to the activities related to the location of the port (existing fishing basins around, an ideal location for tourism, a location at the crossroads of different countries and continents, etc.) and to the different challenges that ports have to face.

The global infrastructure of a port is composed of marine infrastructure (breakwaters, dredging, locks, basins, jetties, quays, mooring piers, etc.), distribution infrastructure (internal roads, railways, walkways, etc.), buildings and terminals managed and maintained by the Port Authority. The port facilities are usually let by the Port Authority to private terminal operators in charge of managing and maintaining the superstructure (such as cranes, silos, specific fencing, control facilities, passenger terminals) to deliver the specific port facility operations.

Besides, various authorities reside in ports facilities to provide services, controls and inspections related to ship and port operations (see 3.3).

A port can address three main categories of activities, to which infrastructures and services are adapted:

- **Activities related to maritime cargo** (container, general cargo, liquid or dry bulk, etc.) with dedicated infrastructure and services to welcome cargo vessels and manage related operations (e.g. unloading and loading, storage, customs inspection, sanitary controls, etc.).

- **Activities related to passengers and vehicles transport** with dedicated infrastructure and services to welcome passengers and vehicles on ships and manager related operations (e.g. passenger gangways, parking, restaurants and bars, border control, etc.). This includes RoRo (Roll-on/roll-off ships) activity as cargo is on trucks.

- **Activities related to fishing** with dedicated infrastructure and services to welcome fishing boats and manage related operations (e.g. fish unloading/loading, fish inspection, fish refrigerated storage, etc.)

In order to support these various activities, the port provides main services, represented in the Figure 2: Port services and infrastructure and detailed in Table 1: Detailed port services. These services are grouped into seven categories, which were defined based on the desktop research and information provided by the experts who contributed to this report.
### Table 1: Detailed port services

<table>
<thead>
<tr>
<th>Service category</th>
<th>Service description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vessel berthing services</td>
<td>When a vessel arrives and leaves a port, different services are provided: berth allocation, marine pilotage, ship supplies such as refuelling or food supply, towing, mooring, vessel safety and security management, bulk water management, services to the crew, ship repair, etc.</td>
</tr>
<tr>
<td>Vessel loading and unloading services</td>
<td>When a vessel is berthed in a port, different services are provided to load and unload freight, fishes, passengers and vehicles: quay cranes and conveyor belts operations, pumping, freight tracking, passenger gangways set up, access controls at boarding, safety and security, operations monitoring, etc.</td>
</tr>
<tr>
<td>Temporary storage and staying services</td>
<td>When freight or fishes are on quays, temporary storage services are provided before they are distributed and transferred, depending on the nature of the freight: container moving, storage and stacking; bulk solids conveyor belts operations and storage; grain conveyors and silos operations; bulk liquids pumping and reservoirs filling; general cargo storage; refrigerated cargo storage; etc.</td>
</tr>
<tr>
<td>Distribution and transfer services</td>
<td>In a similar way, staying services are provided for vehicles and passengers: parking, passenger lounges, luggage handling facilities, restaurants and bars, shopping malls, etc.</td>
</tr>
<tr>
<td>Distribution and transfer services</td>
<td>To ensure the hinterland connectivity, distributing and transferring services are provided: inland port services, train stations and marshalling yards, passenger and luggage controls, intermodal transport hubs, container scanning, port entry and exit, etc.</td>
</tr>
<tr>
<td>Support services</td>
<td>To support the services describing above, the Port Authority or other private companies provide the following service: freight tracking, maritime traffic control, land and infrastructure management, real estate and facility management, terminal operations management, berthing and pilotage management, dangerous goods management, maintenance, port operations management, port administration, etc.</td>
</tr>
</tbody>
</table>
2.3 OVERVIEW OF KEY STAKEHOLDERS
The panorama of the stakeholders involved in port operations and processes is complex and is accentuated by the considerable differences in governance and functioning that may exist between European ports. However, a high-level overview can be drawn to differentiate categories of stakeholders by macro roles, based on the desktop research and information provided by the experts who contributed to this report.

Figure 3: Overview of port stakeholders

2.4 HIGH-LEVEL REFERENCE MODEL
The complexity and the diversity of the port ecosystem (various operational and economic models, different governance, large typology of stakeholders involved, responsibilities shared between stakeholders, etc.) and the unicity of each port are reflected in a very diverse approach to information and operational technology (IT/OT) systems management. Indeed, from one port
to another, IT and OT systems are not the same, are not operated and managed by the same types of stakeholders and not implemented in the same way.

This report provides a high-level reference model based on the desktop research and information provided by the experts who contributed to this report. Its objectives are to list, from a high-level perspective, the main port systems, data flows and interactions with external systems. However, this model must be nuanced and adapted, because it cannot fully correspond to the specificities of each port. For instance, the Port Community System functionality differs between ports, depending on their specific activities and services as well as their overseeing authorities.

Figure 4: High-level reference model of the port systems

2.4.1 Description of the systems
The high-level reference model represents the port systems (block in the middle), and the third parties’ systems interacting with them.

Third parties’ systems are grouped into 4 main categories: systems used by maritime stakeholders’ (shipping companies, ship agent, ship master and crew, etc.), systems used by other transport stakeholders to share freight or passenger information and enable the transhipment (inland waterborne transport companies, roadway companies, railway companies, etc.), systems used by authorities at local, national and European levels and systems used for satellite and maritime surveillance.

Regarding port systems, they are regrouped into two main categories:
- **exchange data systems of the port community** for vessel, fishing or freight related services, especially used as central point for data exchange with shipping companies, also called “single window”;
- **port management information systems**, that includes maritime traffic control systems, corporate systems (emails, ERP, etc.), security and safety systems as well as Terminal Operation Management Systems, often owned by private companies.

### 2.4.2 Description of data flows

Port systems interact with a wide range of systems through machine-to-machine interconnections or manual ones (with information exchanged though web interfaces, by phone calls, emails, paper or fax).

A large amount of data is exchanged between the port and the different stakeholders, which is classified into 5 categories according to this reference model:

- the **mandatory declarations** (information that shipping companies or other stakeholders must report to the Port Authority or other authorities, with respect to the international, European and national legislations);
- the **control and authorisation** given by the authorities to the commercial stakeholders (*e.g.* authorisation to access to the port, authorisation to unload the goods);
- the **operational data** related to the port services and processes (*e.g.* needs for ship refuelling, scheduling of cargo operations);
- the **financial data** (*e.g.* invoicing from the port to its client, payment); and
- the **navigation data** (*e.g.* GPS position of a ship in the port area, AIS data).
3. PORT ASSET TAXONOMY

3.1 ASSET TAXONOMY OVERVIEW

To identify cyber threats associated to the port ecosystem, it is essential to start from identification and breakdown of the port’s assets. Figure 5 provides an overview of the main asset categories that could be found in a port and details the assets for each category: this taxonomy should not be considered as comprehensive; it aims at representing the main assets and doesn’t reflect the diversity and the specificities of different ports. Table 3 describes each asset represented in the asset taxonomy.

Ten asset categories are identified based on the desktop research and information provided by the experts who contributed to this report: the fixed infrastructure, the mobile infrastructure, the OT systems and networks, the OT end-devices associated, the IT systems, the IT end-devices associated, the networks and communications components, the safety and security systems, the information and data, and the people.
Figure 5: Asset taxonomy

ASSET TAXONOMY

MOBILE INFRASTRUCTURE
- Post-service ships
- Special vehicles
- Physical floating barriers

FIXED INFRASTRUCTURE
- Seaside connectivity
- Port infrastructures
- Buildings
- Energy
- Waste treatment systems
- Hinterland connectivity
- Safety & security

OT SYSTEMS & NETWORKS
- Port Community Systems (PCS)
- Cargo Community Systems (CCS)
- Fisheries Information Management Systems (FIMS)
- Port Corporate Systems
- Terminal Operations Management Systems
- VTS/VTMIS
- Berth Management Systems

OT END-DEVICES
- Port Facility specific lay-out
- Vessels berthing
- Vessels loading and unloading
- Temporary storage
- Hinterland connectivity

IT SYSTEMS
- Detection systems
- Emergency communication systems
- Access control systems
- Traffic monitoring systems
- Surveillance & Inspection systems
- Evacuation systems
- Identification systems
- Alerting systems

SAFETY & SECURITY SYSTEMS
- Mandatory declarations
- Commercial & financial data
- Navigation data
- Control & authorisation
- Operational data

PEOPLE
- IT authority staff
- Permanent commercial staff
- IT/OT staff
- External staff
- Ship crews
- Passengers
- General public

INFORMATION & DATA
- Workstations, walls of screens etc.
- Mobile devices

NETWORK & COMMUNICATION COMPONENTS
- Radio
- Protocols
- Servers
- Networks
- Switches
- Routers
- Cables
- LAN, VLAN
- Network security
- Cloud
### 3.2 DESCRIPTION OF PORT ASSETS

#### Table 2: Description of port’s assets

<table>
<thead>
<tr>
<th>Sub-categories</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fixed infrastructure</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Seaside connectivity</strong></td>
<td>Those assets are related to the navigation between the seaside and the port area to ensure that the vessels can enter and exit the port: breakwaters, sea locks, buoys, light beacons, marking of waterways, tide, wind and currents monitoring, radar monitoring of waterways.</td>
</tr>
<tr>
<td><strong>Portuary infrastructure</strong></td>
<td>The assets are related to the mooring of the vessels in the port (docks, quays, jetties, piers), the lighting, the access control (gates, plate reading systems, detectors) and the transport inside the port areas (roads, railways, waterways, walk roads).</td>
</tr>
<tr>
<td><strong>Buildings</strong></td>
<td>The port buildings host the different offices related to the port services (Harbour Master office, customs office, etc.) and the data centres hosting all the IT and OT systems.</td>
</tr>
<tr>
<td><strong>Energy</strong></td>
<td>Those assets are related to the supply of energy for the port ecosystem (buildings, vessels, etc.): electricity network (with high-voltage for large ports), fresh water bunkering and delivery stations, pipeline, fuel, petrol, etc.</td>
</tr>
<tr>
<td><strong>Waste treatment systems</strong></td>
<td>The port manages not only its waste but also the waste of the vessels (solid waste such as plastic, paper, glass, food and liquid waste such as bilge water, sludge and sewage).</td>
</tr>
<tr>
<td><strong>Hinterland connectivity</strong></td>
<td>The port, as an interface between the sea and the hinterland transport systems, has hinterland connectivity assets such as railway stations and rolling stock loading and dispatch systems, road infrastructure, intermodal stations, canals and port infrastructures connecting with inland waterways.</td>
</tr>
<tr>
<td><strong>Safety &amp; security</strong></td>
<td>The port has also dedicated infrastructure to ensure safety and security: control tower, operational room, security centre, first response facilities (firefighting, pollution, containment, evacuation routes, medical facilities, etc.).</td>
</tr>
<tr>
<td><strong>Mobile infrastructure</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Port service ships</strong></td>
<td>The port has dedicated service ships at disposal to deliver specific services on water to the vessels: pilot boats, tugboats, boatage and mooring assistance, supply vessels, safety vessels, inspection and security vessels.</td>
</tr>
<tr>
<td><strong>Special vehicles</strong></td>
<td>Identically, the port has dedicated vehicles at disposal to deliver inland services: firefighting, ambulance, mobile cargo control units, etc.</td>
</tr>
<tr>
<td><strong>Physical floating barriers</strong></td>
<td>To protect other critical vessels and port areas, to contain pollutions and other purpose, the port can use physical floating barriers.</td>
</tr>
<tr>
<td><strong>OT systems and networks</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Industrial control systems (ICS)</strong></td>
<td>In the port, there are different Industrial Control Systems (ICS), for managing port access and vessels berthing (bridges, locks, gates, etc.), port infrastructure (buildings, etc.) and terminal operations (cranes, storage, etc.). The ICS is composed of the following components: automatons and analysers (PLCs, RTUs), databases (Historian, MES, etc.), supervisory systems (DGS, SCADA), HMI / workstations (programming consoles, engineering workstation), Maintenance systems and Safety Instrumented Systems (SIS).</td>
</tr>
<tr>
<td><strong>Communications networks &amp; components</strong></td>
<td>To ensure the communications between the ICS components, the port manage the following assets: switches (managed and unmanaged), wireless access points, protocols, power supply systems (water, electricity, etc.)</td>
</tr>
<tr>
<td><strong>OT END devices</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Related to port facility specific lay-out</strong></td>
<td>The end-devices of the ICS related to the port facility specific lay-out are: specific fencing and access control, specific safety and security equipment, first response equipment, specific operational room, etc.</td>
</tr>
<tr>
<td><strong>Related to vessels berthing</strong></td>
<td>The end-devices of the ICS related to the port vessels berthing are: boatage, berth management systems, specific inspection and control equipment, etc.</td>
</tr>
</tbody>
</table>
### Related to vessel loading and unloading

To load and unload the vessels, many OT end-devices are used: terminal-specific handling equipment and systems (cranes, ramps for passengers, pipelines, belt, conveyors, etc.), terminal-specific freight tracking systems (barcodes, liquid meters, RFID, seals, scales etc.), people badge or ticket scanners, plates reading systems, fault detectors in automated loading/unloading systems (leakages, shocks, jamming etc.)

### Related to temporary storage

Once the cargo or container are out of the vessel, they are temporarily stored in the port areas, different OT end-devices are used: internal transport systems (straddle carrier, yard, truck, chassis, etc.), storage equipment systems (pallet racks, tankage, etc.), cooled and uncooled stores, silos, tanks, switches (managed and unmanaged) for pipes and conveyor belts, wireless access points for « smart » seals and container self-localisation devices, etc.

### Related to hinterland connectivity

To get in or out the cargo, container, vehicles or passengers, different end-devices are used to control and inspect them, and then transport them to other transport systems: control and inspection systems (scanners, inspection systems, Xray), railway station, marshalling yards for wagons, multimodal transport hubs for people (passengers, workers…), inland port facilities, port gate control equipment (plates reading, badges, barcodes reading, detectors)

### IT systems

#### Port Community System (PCS)

The Port Community System is usually owned and managed by the Port Authority or port stakeholders, increasingly organised, as a single window system to share information on port operations related to the vessels between all the port stakeholders (date of arrival or departure of the ship given by the shipping companies, mandatory declarations such as crew list, dangerous goods declarations, bookings of vessel services, etc.).

#### Cargo Community System (CCS)

The Cargo Community System is usually owned and managed by port stakeholders that are usually private companies in charge of the terminal port operations. This system is used to share information on port operations related to the cargo and containers between all involved stakeholders (content of the cargo, localisation of a container, hour of its transfer, customs declarations, etc.).

#### Fisheries Information Management System (FIMS)

For ports hosting fishing activities, the FIMS, as an integrated collection of applications and processes, is owned by the local fisheries authority and used by port stakeholders to manage fisheries operations (loading and unloading), traceability of fish catches, catch certifications.

#### Port Corporate Systems

The Port Corporate Systems are composed of different applications, systems, workstations and servers, common to every companies: financial, human resources (HR), communication and networks systems, emailing systems, sales and marketing systems (ERP), etc.

#### Terminal Operations Management Systems

The Terminal Operations Management Systems, usually owned, used and maintained by private terminal operators, are mainly composed of different systems: enterprise operations systems to plan and manage the logistics and operations (ERP, CRM, etc.), the OT systems specific to the terminal operations (cranes, etc.), terminal operating systems (TOS) used to optimise the logistics, transhipment and warehouse systems.

#### VTS/VTMIS

A Vessel Traffic Service (VTS) is a marine traffic monitoring system. The Vessel Traffic Management Information System (VTMIS) is an extension of the VTS which integrates other information and functionalities to increase the effectiveness of port operations (allocation of resources, etc.).

#### Berth Management Systems

Those systems are used by Port Authorities to manage and ensure safety in mooring processes: warnings and alerts, meteorological data, video cameras streams, berth allocation management, etc.

### IT END-devices

#### Workstations

Different workstations are used in ports: dedicated to IT systems, dedicated to OT systems, to maintenance, mobile and fixes workstations, etc.

#### Mobile devices

Different mobile devices are used in ports: smartphones, tablets, TETRA radios, specific devices used for logistics (scanning, etc.) etc.

---

40 The governance of PCS is complex and differs from one port to another. For instance, the PCS of the ports of Rotterdam and Amsterdam were merged to create a unique one, receiving a license to operate from the port communities of Amsterdam and Rotterdam and becoming the PCS of Dutch ports. See [https://www.portbase.com/en/about-us/](https://www.portbase.com/en/about-us/)

41 The governance of CCS is also complex and differs from one port to another and from one Member State from another. For example, due to the French regulations, although closely connected, the PCS and CCS are different systems with specific governance: the CCS is operated by private companies (operated by SOGET for different French ports such as Le Havre). Whereas, in other countries, to use again the example of the ports of Amsterdam and Rotterdam, the CCS is the same system than the PCS. See [http://www.soget.fr/en/soget-siege-3/about-us.html](http://www.soget.fr/en/soget-siege-3/about-us.html)

42 See [http://www.franciscoblaha.info/fisheries-information-systems](http://www.franciscoblaha.info/fisheries-information-systems)
## Networks and communication components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio</td>
<td>Radio systems (RFID, VHF, etc.) are used for many port processes: communication with ships, safety and security operations, logistics management, etc.</td>
</tr>
<tr>
<td>Protocols</td>
<td>Protocols are used to exchange information: EDI, API, authentication protocols, etc.</td>
</tr>
<tr>
<td>Servers</td>
<td>Numerous servers are used in the ports for different uses: web servers, application servers, proxy servers, mail servers, virtual servers, printers, etc.</td>
</tr>
<tr>
<td>Networks</td>
<td>Different networks are set up in ports: VHF radios (Internet, WiMAX/WIFI, Satellite, ad-hoc networks, VLAN/LAN, etc. They can be managed by different stakeholders at different levels.</td>
</tr>
<tr>
<td>Switches, Routers, Hubs</td>
<td>Those components are used to forward packet in different manner between different networks.</td>
</tr>
<tr>
<td>Network security</td>
<td>To protect the network, firewall, IPS/IDS, PKI/MFA, Antivirus, SIEM and other security solutions are set up in the port areas.</td>
</tr>
<tr>
<td>Cloud</td>
<td>Ports can use some Cloud solutions to host some of its data, for example emails and shared folders.</td>
</tr>
</tbody>
</table>

## Information and data

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory declarations</td>
<td>Many declarations are mandatory for a ship to get into the port area, in respect with international, European, national and local regulations. For instance, mandatory by the FAL Convention: passenger and crew, vessel, cargo, border control, waste, security, health, travel information is required.</td>
</tr>
<tr>
<td>Commercial and financial data</td>
<td>As any company, the ports deliver services to companies (shipping companies, etc.) and books different services to their providers (ICT providers for example): financial and commercial are exchanges (money transfer, invoicing, etc.).</td>
</tr>
<tr>
<td>Navigation data</td>
<td>Through satellite and navigation data (AIS, SafeSeaNet, etc.), the different stakeholders share navigation data with the port (GPS position, information on maritime routes, etc.).</td>
</tr>
<tr>
<td>Control &amp; Authorisation</td>
<td>The Port Authorities and other national authorities control and deliver authorisation for vessel and cargo movement.</td>
</tr>
<tr>
<td>Operational data</td>
<td>In order to plan and manage all the services (ship services, logistics services, etc.), operational data are shared between the port stakeholders.</td>
</tr>
</tbody>
</table>

## Safety and security systems

Many systems are set up in the port areas to ensure safety and security of people and port infrastructure:

- Detection systems such as video-surveillance (CCTV), incident management systems, first response centre systems, IDS (intrusion detection systems), abnormal behaviour detection systems;
- Emergency communication systems;
- Access control systems such as automatic gates, smart fencing systems, badging systems, access monitoring and counting systems;
- Traffic monitoring systems such as radar and electro-optic monitoring systems, train and truck traffic monitoring systems;
- Surveillance & inspection systems such as patrolling staff, oats, dogs and vehicles, detectors (fires, gas leaks, nuclear, etc.), X-ray scanners;
- Evacuation systems such as exit route guidance, muster points, guidance screens, emergency doors;
- Identification & authentication systems such as face recognition systems, biometric systems, ID control portable terminals; and
- Alerting systems such as sirens and loudspeakers.

## People

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port authority staff</td>
<td>The Port Authority employs directly people, as statuary staff.</td>
</tr>
<tr>
<td>Permanent commercial staff</td>
<td>The companies operating permanently in the ports employs people, as statuary staff (terminal operators, permanent service providers, etc.).</td>
</tr>
<tr>
<td><strong>IT/OT staff</strong></td>
<td>The IT and OT staff, employed by the Port Authorities and private companies operates in different systems to set up new solutions and maintain them (CISO, CIO, administrations, etc.).</td>
</tr>
<tr>
<td><strong>External staff</strong></td>
<td>Many other people operate in ports: port facility external staff, other service staff (third-parties), temporarily authorized staff (contractors, taxi drivers, etc.).</td>
</tr>
<tr>
<td><strong>Ship crews</strong></td>
<td>When a ship arrives in a port, the crew’s members and their captain can use the different facilities of the port (restaurant, bar, etc.).</td>
</tr>
<tr>
<td><strong>Passengers</strong></td>
<td>The passengers pass through the port areas to go up in the cruise ships and ferries.</td>
</tr>
<tr>
<td><strong>General public</strong></td>
<td>Usually, some port areas are opened to the public (tourism, research, etc.).</td>
</tr>
</tbody>
</table>
4. CYBERSECURITY THREATS AND CHALLENGES

4.1 THREAT TAXONOMY

Ports face numerous cybersecurity challenges, some of them are quite generic within any IT and OT environment, while others are quite specific to port ecosystems. Table 3 identifies the possible impact of cybersecurity incidents for a port.

Table 3: Possible impacts for ports

<table>
<thead>
<tr>
<th>Impacts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown of operations, port paralysis</td>
<td>The shutdown of the port operations is a much-feared impact by the port ecosystem: if it lasts more than a few hours, it can harm strongly the commercial operations (loss of money), the delivery of essential goods for a nation, especially for the islands (food, fuel, etc.) as well as pose safety and security issues (queue of several boats at the port entrance).</td>
</tr>
<tr>
<td>Human injuries or death, Kidnapping</td>
<td>Ports must face high security and safety challenges, because many people work in port areas can perform dangerous jobs (manipulation of cranes, of dangerous goods, etc.) and because ports also must manage a quite large passenger flow easy to predict (ferries, large cruise vessels, etc.).</td>
</tr>
<tr>
<td>Sensitive and critical data theft</td>
<td>Port systems may hold critical information, whether it is personal information (crew or passenger data), critical commercial information (location and content of containers, competitive know-how) or National security information (port being essential assets for a nation): the theft of these information can have disastrous consequences.</td>
</tr>
<tr>
<td>Cargo and goods stealing</td>
<td>Attackers can browse cargo and container lists to identify the most valuable goods for black markets (to be stolen in the port or targeted for future piracy attacks when the ship in at sea).</td>
</tr>
<tr>
<td>Illegal trafficking</td>
<td>The marine ecosystem is one of the largest playgrounds for organized crime: ports are often used for illegal and criminal traffic (drugs, arms, prohibited goods, most wanted people...).</td>
</tr>
<tr>
<td>Financial loss and costs</td>
<td>A port can lose a lot of money due to the stop of operations or for repair budget, in case of damage on its systems and infrastructure</td>
</tr>
<tr>
<td>Fraud and money steal</td>
<td>As any major company, the financial systems of the ports can be compromised to steal money from them. Indeed, especially for the biggest ports, the port revenues are important: for example, the Port of Rotterdam Authority’s revenue, in 2017, was € 712.1 million. Moreover, since ports are the border between two States or continents, fraudulent companies can falsify their customs declarations (VAT fraud).</td>
</tr>
<tr>
<td>Systems damages or worst, destruction</td>
<td>Due to the high complexity of port systems and infrastructure, some of which are critical (e.g., industrial systems that manage large amounts of dangerous goods), damage or worse, destruction to those systems and infrastructure has disastrous consequences for port operations and safety and security, including people. Tankers (especially refined products and gas) are very vulnerable to fire and explosion; local storage of flammables and chemicals is also possibly massive.</td>
</tr>
<tr>
<td>Tarnished reputation, loss of competitiveness</td>
<td>Nowadays, ports are in an extremely competitive international ecosystem: the slightest incident or problem on its activities and operations can damage its reputation and lose customers who could direct their traffic to neighbouring ports.</td>
</tr>
</tbody>
</table>
As the port is the direct interface between the hinterland and the sea, an environmental disaster in port areas can have disastrous consequences on populations, fauna and flora and human infrastructure, at a very long distance (oil spill, gas explosion, ocean pollution, shipwrecks, etc.).

Finally, main threats that port ecosystems can be exposed to are described in Figure 6: Threat taxonomy and detailed in the Table 4: Threat description.

**Figure 6: Threat taxonomy**

![Threat Taxonomy Diagram](image-url)
## Table 4: Threat description

<table>
<thead>
<tr>
<th>Sub-categories</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Eavesdropping, interception, hijacking</strong></td>
<td></td>
</tr>
<tr>
<td>Interception of emissions</td>
<td>Hackers can intercept the communication between the port and the different stakeholders (radio, exchanges between ships and port, etc.).</td>
</tr>
<tr>
<td>Interception of sensitive data</td>
<td>Communications can be listened, or the systems can be scanned to intercept sensitive data for corporate espionage, state espionage or criminal crime and piracy espionage.</td>
</tr>
<tr>
<td>Man-in-the-middle, session hijacking</td>
<td>In a Man-in-the-middle attack, the attacker relays and possibly alters the communication between two parties who believe they are directly communicating with each other. With session hijacking hacker can exploit systems vulnerabilities to gain the same access rights than the targeted clients (authentication cookies for instance)</td>
</tr>
<tr>
<td>Network reconnaissance and traffic manipulation</td>
<td>The attacker scans the network passively until he can find an entry door which reveals to him internal port network information (open ports, used protocols, etc.). With this knowledge, the attacker operates to compromise the targeted systems.</td>
</tr>
<tr>
<td><strong>Nefarious activity and abuse</strong></td>
<td></td>
</tr>
<tr>
<td>Denial of service (DoS)</td>
<td>A DoS attack can target different systems: RGPS, network, applications, IoT, etc. The objectives of such attack is to lead to system unavailability and production disruption. Most DoS attacks are caused by several sources at the same time (e.g. massive number of requests sent by different systems at the same time) sent to the target system, also called Distributed Denial of Service (DDoS).</td>
</tr>
<tr>
<td>Malware</td>
<td>The penetration of malicious software in the port systems can lead to unwanted and unauthorised actions, exploiting for some of them vulnerabilities to elevate the privileges which may cause damage on port IT/OT systems, infrastructure, data integrity and operations. There are different types of malware created for different purpose: ransomware, viruses, Trojan horses, spyware, injection or web application attacks, etc.</td>
</tr>
<tr>
<td>Brute force</td>
<td>The brute force attack is used for gaining unauthorised access to an organisation's resources (i.e. data, systems, devices, etc.) through many attempts to guess the correct key or password. If the port systems allow the utilisation of simple or defaults passwords, they can be especially vulnerable to this kind of attacks.</td>
</tr>
<tr>
<td>Identity theft</td>
<td>A hacker can use, deliberately, the identity of a person involved in the port ecosystem, through for example the stealing of credentials, to obtain financial gain, critical information, unauthorised access to a system, etc. The “fake president” fraud, using identity of powerful people in the ecosystem, can have serious impact.</td>
</tr>
<tr>
<td>Social engineering, phishing</td>
<td>An attacker can use human interaction to obtain or compromise information about port organization and port processes: by asking questions, by pretending to be another person, the attacker can piece together information he needs to infiltrate the port systems. The attacker can ask several sources, by relying on the information he can get from the first source to add to his credibility or sending malicious links. The phishing attacks is the most common social engineering attack: hackers use email or malicious websites to solicit personal information by posing as a trustworthy organization. Other forms exist: vishing attack (though voice communication), smishing attack (exploitation of SMS, text, messages containing malicious link, etc.)</td>
</tr>
<tr>
<td>Targeted attacks</td>
<td>A targeted attack is a sophisticated and malicious attack specifically targeting the port, designed to infiltrate its systems for different purposes. For instance, the Advanced Persistent Threat (APT) is a stealthy, diffuse and continuous attack over a long period of time designed to integrate malicious code into targeted systems that perform specific tasks without being noticed.</td>
</tr>
<tr>
<td>Abuse and theft of data</td>
<td>The hacker, through different means, steals sensitive data (personal data, freight tracking data, operational data, etc.) and/or abuse the certificates used in the port operations (ship certificates, etc.).</td>
</tr>
<tr>
<td>Manipulation of data</td>
<td>The hacker can manipulate data (financial data, navigation data, freight data, operations, etc.) in the systems to fulfil its objectives.</td>
</tr>
<tr>
<td>Geo-localisation signals spoofing/jamming</td>
<td>The hacker can manipulate geo-localisation and navigation systems to change the trajectory of a vessel provoke accidents for instance. Recent attacks using GPS spoofing and AIS tampering show that this threat is important and must be considered, especially in the maritime context.(^{43})</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>

#### Physical attacks

| Fraud | A fraud is an intentional deception which aims to violate the civil law for different purposes. For example, in the port ecosystem, through fake customs declarations, companies can carry out VAT fraud. |
| Sabotage | A sabotage is a deliberate action realised to deteriorate or destroy the port systems and infrastructure in order to weaken the port ecosystem (mostly for military, political or ideological objectives). The sabotage can be external (from people not directly involved in the port operations) or internal (from people directly involved in the port operations, such as resentful employees, etc.). |
| Vandalism | A vandalism is a voluntary act of destruction or deterioration of port assets without any specific reason. In the port ecosystem, vandalism can be done on port IT and OT systems, ships or other vehicles, and freight (goods, cargo, container, etc.). |
| Theft | An attacker can steal mobile devices (mobile phone, radios, etc.), fixed hardware, backups, printed documents (list of goods, ships, etc.), freight (goods, cargo, container, etc.). |
| Unauthorised access | An attacker can bypass access control systems to enter in the port areas, access to a ship or other vehicles or OT end-devices (cranes, etc.). Moreover, unauthorised vehicles and ships can also entry to the port areas. |
| Terrorism | Terrorism is defined as the use of intentional violence, generally against civilians, for political, ideological and religious purposes |
| Hacktivism | Hacktivism is the use of technology to promote a political agenda or a social change. |
| Coercion, extortion or corruption | Extortion and coercion are defined as the use of violence or threats to obtain something, especially money. Corruption is defined as a dishonest or illegal behavior targeting powerful people in the port ecosystem such as bribery. |
| Piracy, illegal crime, mafia | Piracy, illegal crime and mafia are illegal and unauthorised organizations who break the law to maintain their power and their illegal activities (drug trafficking, cargo theft, etc.) |

#### Unintentional damage

| Use of unreliable source | The use of unreliable source for the port systems (defective update, malicious software, etc.) can cause systems to malfunction or spread. The NotPetya attack is a perfect example of this. |
| Erroneous administration of IT/OT systems | Even with good intentions, if the administrators of port systems are not enough trained and made aware of the impacts of such errors, erroneous administration can impact strongly the port systems, and if they are critical, directly the port operations. |
| Resulting from penetration testing | In order to test the security level of port systems, the port may order penetration testing which, if not carried out properly, could damage the systems. |
| Data deletion | By mistakes, employees or other stakeholders accessing port systems can delete critical information which could have impact on port operations (for instance, freight or navigation information). |
| 3rd party security failure | The port systems are managed and maintained by different service providers: if their accesses are not properly controlled, the security breaches of the 3rd party can directly affect the port systems (in case of maintenance for instance). |
| Information leakage | Employees can share, by mistakes or ignorance, sensitive data if there is an insufficient awareness and data protection solution. |

#### Failures and malfunctions

| Failures or malfunctions of systems or devices | A failure or a malfunction of IT or OT systems or end-devices can occasionally happen, especially if proper maintenance and compliance with the manuals and instructions during the exploitation is not ensured, or if the proper functioning is not measured and monitored regularly. |

\(^{43}\) See https://www.ship-technology.com/features/ship-navigation-risks/
Vulnerabilities

| exploitation of | Systems and devices may have vulnerabilities that could be exploited by hackers, particularly if systems or devices are not patched on time or regularly monitored while corrective measures are put in place in the meantime. |
| systems or devices | |

Failures and
malfunctions of
other stakeholders’
systems

| systems | The systems (navigation, communication and other systems) of other port actors (ships, other transport actors, etc.) may have malfunctions or failures that may lead to the slowing or even stopping of port operations. In addition, if those systems are linked to port systems, an attacker can exploit the vulnerabilities of those systems as an entry door to port systems. |

Main supply systems

| systems | The port is dependent on different supply systems (electricity, fuel, etc.) which are essential to ensure port operations: in the event of failure or interruption of those systems, port operations will be slowed down or even stopped. |

Failure or
disruption of
service providers

| The port is dependent of many service providers, and some of them can be critical for the port operations. A failure or disruption of these service providers can strongly impact the port operations. |

Outages

| Main supply outages | Outages on main supply can have important impacts on the port operations: shutdown on the fuelling supply leads to block the ships in the port; outage on the electricity networks impact the IT and OT systems (for example, no communication possible between the port stakeholders, the refrigerated storage can no longer maintain frozen goods). |
| Network outage | Port networks are essential for port operations and communication between the various actors (Port Authority, terminal operators, ships, other authorities, etc.): failures in port networks can strongly affect their operations. |
| Absence of personnel | An incident could occur in a port area or at a time where port employees are not present and may have significant consequences in port systems and infrastructure, especially in the case of increasing automation of the port processes. |

Disaster

| Environmental disaster | The threat of incident and unfavourable conditions such as fires, pollution, dust, corrosion, explosions, which may cause physical damage to the port assets. |
| Natural disaster | The threat of natural disaster such as floods, lightning strikes, powerful waves, storms, heavy winds, rain, which may cause damage to the port assets. |

4.2 CYBERSECURITY CHALLENGES

Based on the desk research and data from interviews, the main challenges currently faced by ports to implement cybersecurity measures are the following:

- **Lack of digital culture in the port ecosystem**, in which some stakeholders are still conservative. Indeed, new trends such as digitisation and IoT initiatives are colliding with the conservative nature of the maritime industry, but are becoming more and more adopted. In this context, the cyber security needs and best practices of these initiatives are often not considered as a priority by stakeholders who are first looking at technology adoption;
- **Lack of awareness and training regarding cybersecurity**: ports ecosystem used to only rely on safety and physical security to address risks, IT and OT bring new challenges with regards to cybersecurity that port stakeholders often do not fully anticipate and master;
- **Lack of time and budget allocated to cybersecurity**: as a consequence of poor awareness, especially of top management with regards to cybersecurity challenges;
- **Lack of human resources and qualified people regarding cybersecurity matters**: the ports do not have enough people in IT and OT staff to manage all projects, especially cybersecurity projects. Moreover, cybersecurity skills are very specific and scarce which makes it difficult for small companies to hire adequately qualified people on those topics;
• Complexity of the port ecosystem due to the number and diversity of stakeholders taking part in port operations: stakeholders within a port can be numerous (up to 900 for the biggest ports). This ecosystem is built from companies of various sizes, with various levels of cybersecurity capabilities and can even be direct competitors among themselves. This makes the overall cybersecurity control at port level difficult with heterogeneous level of controls within the port. \(^4^4\)

• Need to find a right balance between business efficiency and cybersecurity, especially by guaranteeing the continuity of services while keeping IT and OT secure, such as disconnecting critical systems and updating systems without any business impacts;

• Legacy of some systems and practices: especially regarding systems managing navigation data and OT systems which can be very old and vulnerable and for which extra cybersecurity measures must be enforced;

• Lack of regulatory requirements regarding cybersecurity: the NIS Directive is a first base to implement cybersecurity measures, but only concerns some of the stakeholders in the maritime sector. This is not yet enough to ensure a proper level of cybersecurity over the entire port ecosystem and to allow enough budgets to be released to meet the requirements; and

• Difficulty to stay up to date with the latest threats, especially in view of the diversity of stakeholders operating in the ports, the processes, the systems implemented and used and the rapid growth of innovations in the port ecosystem;

• Technical complexity of port IT and OT systems: the port stakeholders use different systems that are developed, managed and maintained by different teams or entities. For example, they can be developed either by port IT teams, either by third-parties or by IT providers. Moreover, they can be based on various technologies. Finally, teams managing the security of IT and OT systems can also be different. Therefore, the mapping of all port systems is difficult to define and to maintain overtime;

• IT and OT convergence and interconnection: Usually OT systems, more vulnerable than IT systems, are protected because they are separated from IT systems and networks. But, increasingly, IT and OT systems and networks, become more and more dependent and interconnected, exposing OT systems to higher risks;

• Supply chain challenges. A number of cybersecurity challenges are associated with the supply chain: lack of cybersecurity certifications for port products and services, security risks related to supplier remote access to the port networks/systems, long patching cycles for certain types of systems (e.g. ICS), heterogeneity and high number of supplier landscape, difficulty to change supplier services. Contractors do not have much control over the cybersecurity level of their suppliers and, consequently, over the cyber risks they involve (supply chain attacks);

• Strong interdependencies between port systems and services and external services from other sectors (e.g. energy) that introduce interdependency cybersecurity risks; and

• New cyber risks resulting from the digital transformation of ports: ports are currently launching several projects to digitalize port processes, in particular with the emergence of the SmartPort concept\(^4^5\), cyber risks should be taken into account in the initial phases of those projects.

---

\(^4^4\) See: Port Management Information systems towards privatization. Nam Kyu PARK, Hyung Rim CHOI, Chang Sup LEE, Moo Hong KANG, Jae Woo YANG

\(^4^5\) See SmartPort definition: http://parisinnovationreview.com/articles-en/what-is-a-smart-port
4.3 DESCRIPTION OF KEY CYBERATTACK SCENARIOS

Based on the asset and threat taxonomies listed in sections 3.1 and 4.1, the desktop research as well as the information provided by the experts who have contributed to the report, several cyber-attack scenarios were defined in correlation with the sources of threats and the possible impacts on port assets, listed and detailed in section 4.1. Each scenario is associated with a list of security measures, detailed later in Chapter 5, that will mitigate the risk of this scenario occurring. The security measures are formalised in the form of, to take one example, “TP-01: Network segmentation”, with “TP” as the group of the measures (in this case “Technical Practices”), the associated number (in this case “01”) and the name of the measure (in this case “Network segmentation”).

Scenario A – Compromising of critical data to steal high value cargo or allow illegal trafficking through a targeted attack

This scenario is a sophisticated and targeted attack on port systems (Advanced Persistent Threat): attackers must have in-depth knowledge of port systems and networks (social engineering, network scan), port processes and port infrastructure (physical intrusion) to perform cargo and container theft. An example of such an attack occurred at one of Antwerp’s port terminals in Belgium.

**Figure 7:** Compromising of critical data to steal high value cargo or allow illegal trafficking scenario

| 1 | Gathering information (social engineering) |
| 2 | Identification of targeted systems |
| 3 | Phishing attack to retrieve credentials |
| 4 | Access to cargo and container information |
| 5 | Theft of cargo information |

**Impacts**

- Cargo and goods stealing
- Illegal trafficking
- Tarnished reputation

**Assets affected**

- Cargo Community Systems (CCS)
- Networks
- Email
- People

**Stakeholders involved**

- Terminal Operators
- Police
- Shipping and maritime freight companies
- Senders and consignees

Attack details

- On the one hand, attackers identify and retrieve authentication data (credentials) to get access to useful systems:
  - Attackers gather information on port systems through social engineering
  - Then they identify the targeted systems used for cargo and container management and identity of the people using them
  - Once systems and their operators/users are identified, attackers launch phishing attacks to retrieve credentials to access to those systems
- On the other hand, attackers install components to gain access remotely to the port network and bypass network security:
  - Attackers scan the port networks to find vulnerabilities to exploit them and gather information
  - They install, if necessary, through physical intrusion, components to access remotely to the port networks (wireless access point)
  - To ensure constant access and adapt to each network and infrastructure changes in the long term, they spy on networks
- Attackers have now access to the freight tracking systems and other relevant port systems and they can access critical information on containers they want to steal (localisation, content, pick-up code, etc.) from outside of the port facilities.
- Attackers can then steal the cargo before the official pickup date

Main security measures

- OP-10: Security awareness raising program
- OP-16: Creation of a Cybersecurity Operations Centre (SOC)
- TP-01: Network segmentation
- TP-02: Regular network scans
- TP-08: Multi-factor authentication

Scenario B – Propagation of ransomware leading to a total shutdown of port operations

This scenario can be a targeted or a non-targeted attack (as collateral damage of targeted attack on other companies through the ransomware propagation): the hackers can develop a ransomware exploiting different vulnerabilities to spread it into the port networks and encrypt the different systems and devices (workstations, servers, etc.), leading to the destruction of the infected systems and the potential loss of backups (within servers which could be encrypted). An example of a destructive ransomware-like malware attack was the large-scale incident affecting the operations of Maersk\(^47\).

\(^47\) http://fortune.com/2017/06/27/maersk-petya-ransomware-cyber-attack/
Figure 8: Propagation of ransomware leading to a total shutdown of port operations scenario

**Impacts**
- Tamished reputation
- Financial loss and costs
- Systems damage, or worst, destruction
- Shutdown of port operations, port paralysis

<table>
<thead>
<tr>
<th>Assets affected</th>
<th>Stakeholders involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT systems</td>
<td>All port stakeholders</td>
</tr>
<tr>
<td>OT systems and networks</td>
<td></td>
</tr>
<tr>
<td>OT end-devices</td>
<td></td>
</tr>
<tr>
<td>People</td>
<td></td>
</tr>
<tr>
<td>Information and data</td>
<td></td>
</tr>
</tbody>
</table>

**Attack details**
- The port updates one of its servers with a compromised update (ransomware) – other ways can be used to introduce a ransomware on port systems, for example social engineering (phishing or USB-drop for example) or bad network segregation (wide exposure to the Internet)
- The ransomware spreads into the port’s network, using some unpatched vulnerabilities and lack of network segmentation;
- The ransomware is executed on port’s systems and devices and steal stored credentials
- The ransomware executes a mechanism of elevation of privileges, using bad segregation of highly privileged accounts
- The ransomware spreads into other part of the port’s network by the same mechanism
- The infected systems and devices are encrypted and cannot be used anymore
- A ransom is required while all the systems and devices are down

**Main security measures**
- OP-01: Endpoint protection strategy
- OP-05: Define a vulnerability management process
- OP-16: Creation of a Cybersecurity Operations Centre (SOC)
- TP-01: Network segmentation
TP-13: Privilege Account Management (PAM)
TP-15: Anti-malware and anti-virus management
TP-23: Update management process
TP-24: Source of update verification
PS-15: Ensure cyber resilience of port systems
PS-17: Define a crisis management organization

Scenario C – Compromise of Port Community System for manipulation or theft of data

This scenario is a targeted attack on the systems used for the exchanges between all stakeholders (usually the Port Community Systems). The objectives are to falsify the information on port services to disrupt the operations or to modify some operations in the systems (implying financial loss for the port). This scenario is realistic because those systems are exposed to all port stakeholders by different ways (usually using different networks and systems, through VPN access, or through the Internet, most of the time via machine-to-machine interconnections). Indeed, those systems are increasingly automatically interconnected with external systems (via API, EDI exchanges, etc.): third parties’ systems thus become an additional attack surface to reach port systems.

Because these systems are different from one port to another, there can be multiple ways to set up this attack: for example, if the Port Community Systems are exposed through a web application, the attacker can exploit common vulnerabilities of web applications; if it is an application developed internally by developers employed by the port and if standard security development rules are not applied, specific vulnerabilities can be exploited; etc.

Figure 9: Compromise of Port Community System for manipulation or theft of data scenario
### Impacts

- Financial loss
- Disruption of port operations
- Accident (related to Dangerous goods management)

<table>
<thead>
<tr>
<th>Assets affected</th>
<th>Stakeholders involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Community Systems (PCS)</td>
<td>Port Authority</td>
</tr>
<tr>
<td>Finance systems</td>
<td>Port Terminal Operators</td>
</tr>
<tr>
<td>ERP</td>
<td></td>
</tr>
</tbody>
</table>

### Attack details

- Depending on the PCS architecture and network exposition:
  - If the PCS is exposed to third parties through a dedicated web interface, the attacker can exploit common web application vulnerabilities to have access to the PCS (SQL injection, brute force attack, exploitation of bad access rights segregation, etc.);
  - If the PCS is automatically connected with external systems through data exchanges protocols such as API or EDI protocols, the attacker can organise a man-in-the-middle attack by intercepting the data exchanges and modifying them in case data exchanges are not secured enough;
  - Or if direct access to the PCS itself out of the port network is possible, the attacker can exploit weak network security measures to have direct access to this system and use credentials he may have stolen through social engineering;
- Once the attacker has non-authorised access to the PCS with enough access rights, he can manipulate data directly to the PCS (modification of the port operations, theft of critical data, deletion of data on some operations, etc.)
- The loss of integrity of the PCS data has many consequences: chaos in port operations, potential financial loss for the port that loses information on operations preventing it from invoicing the operations carried out or even accident if data related dangerous goods are manipulated or made unavailable.

### Main security measures

- PS-09: Project methodology including security assessments and checkpoints
- OP-11: Strict control of third parties’ accesses
- OP-16: Creation of a Cybersecurity Operations Centre (SOC)
- OP-17: Regular network scans
- OP-18: Perimeter security with filtering policy
- OP-19: Perform regular cybersecurity audits
- TP-01: Network segmentation
- TP-05: Identity & Access Management (IAM) strategy
- TP-08: Multi-factor authentication
- TP-19: Secure mechanisms for machine-to-machine exchanges
- TP-25: Log correlation and analysis systems

---

**Scenario D – Compromise of OT systems creating a major accident in port areas**

This scenario is specific to the OT world and the ICS specificities and is considered to be realistic even no such attacks in ports are publicly known. Indeed, similar attacks occur in other...
critical sectors, especially in the energy sector. This kind of attack doesn’t need to be generally sophisticated to be impactful and the major risks remain the connection with external networks and systems, especially the Internet. The specificities of such attacks are the close link between the physical and logical world: the attack usually begins in the logical world (from the IT component) and has impacts in the physical world (damage to OT systems and end-devices, safety and security incidents, etc.).

A port contains various OT networks, systems and end-devices used for different services and operations and owned, managed and maintained by different stakeholders: cranes for vessel loading and unloading in port terminals, bridges at the entry of the port to get vessels in and out, systems in refrigerated warehouses to keep fragile foods at a safe temperature, the sensors and systems used to transport, store and monitor dangerous goods, etc.

**Figure 10:** Compromise of OT systems creating a major accident in port areas scenario

---

**Impacts**

- Shutdown of port operations, port paralysis
- Systems damages, or worst, destruction
- Human injuries or death
- Financial loss and costs
- Tarnished reputation and loss of competitiveness
- Environmental disaster

**Assets affected**

- OT systems and networks
- OT end-devices
- Mobile infrastructure
- Fixed infrastructure
- People

**Stakeholders involved**

- Port Authority
- Port Terminal Operators
- Service providers
- Delivery chain

---

### Attack details

- A maintenance laptop accessing OT control systems is compromised with a malicious code (either through compromised USB drive or email, download of malicious software from the Internet, etc.)
- The malicious code is spreading onto the OT networks and then the OT systems when the laptop connects to it
- If the Industrial Control Systems (ICS) are sophisticated (IoT, remote server, etc.), the attackers can deploy mechanisms to command the ICS remotely
- If not, the ICS code is modified to execute predefined commands contained in the malicious code
- The OT end-devices, such as cranes or bridges, move erratically or unexpectedly
- This can cause security and safety incident leading to damage or destruction of port infrastructure, injury or death, etc.

### Security measures

- OP-01: Define an endpoint protection strategy
- OP-09: Develop specific and mandatory cybersecurity training courses for some key population
- OP-12: Clearly define all relevant aspects of the partnership with third parties, include security measures
- OP-16: Creation of a Cybersecurity Operations Centre
- OP-21 and OP-22: IT and OT physical protection
- TP-11: Installation and configuration policy
- TP-14: Dedicated administration network
- TP-30: Network segmentation between IT and OT systems
- TP-29 and TP-31: Consider OT and IoT systems into all the security measures and set up specific security measures
- TP-25: Log correlation and analysis systems
5. SECURITY MEASURES

5.1 SECURITY MEASURES CATEGORIZATION

Development of security measures for ports was one of the focal points of this study. The objective is to provide guidelines and recommendations for Port Authorities, private companies operating in ports and other stakeholders involved in the port ecosystem to help prevent or properly respond to potential cyberattacks on the port systems.

To define the categorisation of these measures, the study relied on identified cyberattack scenarios in part 4.3 as well as security measures from policies and standards listed in section 2.2.2 and common frameworks for cybersecurity like the Reference document on security measures for Operators of Essential Services\(^ {49}\), ISO 27001/2\(^ {50}\) or NIST\(^ {51}\).

Finally, a list of 22 security domains have been defined to classify all security measures in relation with ports. To organise the domains in a logical manner, they were classified into three main groups:

- Policies
- Organisational practices
- Technical practices

As the target audience of this report is eligible to fall under the provisions of the NIS Directive as Operators of Essential Services, the following measures have been developed to map to the measures proposed in the Reference document on security measures for Operators of Essential Services. Still, a few exceptions do exists, most notably Cloud security, Machine-to-machine security and OT & Industrial control systems security, which indicates that a more sector-focused approach may be pertinent to address the specificities of the maritime/port sector.

5.2 POLICIES

It is essential that ports define policies and governance in regard to IT and OT, enforcing cybersecurity best practices, especially for most critical assets, with a risk-based approach.

5.2.1 Security policy and organisation

Security measures to implement and maintain up-to-date an information system security policy (ISSP)

- PS-01: Write and implement an information systems security policy (ISSP) which describes all organisational and technical means and procedures, including topics related to the OT environment. This ISSP must be approved by the port’s top management team to guarantee the high-level endorsement of the policy. Key elements of the ISSP can be integrated in the Port Facility Security Plan required by the ISPS Code.
- PS-02: Enforce security governance of both IT and OT environments through the ISSP by describing the roles and responsibilities of each stakeholder (Port Authority, terminal operators, service providers, suppliers, etc.).


\(^ {50}\) See [https://www.iso.org/isoiec-27001-information-security.html](https://www.iso.org/isoiec-27001-information-security.html)

\(^ {51}\) See [https://www.nist.gov/cyberframework](https://www.nist.gov/cyberframework)
• **PS-03:** Share this ISSP with all stakeholders involved in port operations, or, if more relevant a light version underlying each party responsibilities towards cybersecurity at port level.
• **PS-04:** Review annually the ISSP by considering the results of cyber security tests and risk analysis to tackle new threats and risks.

### 5.2.2 Risk and Threats Management

Security measures to identify and manage continuously risks and threats related to the port ecosystem.

• **PS-05:** Adopt a risk-based approach to build the port cybersecurity strategy and set up a continuous improvement process to ensure that the risks identified are under control and that new risks are properly identified in a timely manner. Ensure identified cyber risks are considered in safety and security plans to align cybersecurity with physical security and safety (in particular, through the Port Facility Security Assessment required by the ISPS Code).
• **PS-06:** Conduct and regularly update risk analysis to identify risk and threats related to the port ecosystem. In particular, risk analysis must be conducted for new projects (SmartPort initiatives such as Big Data, IoT, blockchain, etc.).
• **PS-07:** Set up security indicators and assessment methods to evaluate the compliance of the port systems and processes to the ISSP and risk management performance, by involving several stakeholders when relevant.\(^{52}\)
• **PS-08:** Set up a threat intelligence process to watch continuously for vulnerabilities, identify new risks and threats and deploy actions to mitigate them.
  
  *This measure can be improved by developing collaborative private-public initiatives of sharing information on threat intelligence at European level.*\(^{53}\)

### 5.2.3 Security and privacy by design

Security measures that should be applied from the first stages of systems development and during the development lifecycle in order to increase by design the security levels of any solutions and applications, to protect critical data and ensure the privacy of personal data.

• **PS-09:** Develop a project methodology including security assessments and checkpoints, including for agile projects (risk analysis, architecture security review, security tests, security approval, etc.) for new and existing projects, considering the criticality and exposure of the system. More specifically, strongly include cybersecurity issues in SmartPort projects from the design stage to implementation.
• **PS-10:** Address privacy related issues based on applicable local and international regulations, such as the General Data Protection Regulation (GDPR).\(^{54}\)
• **PS-11:** Launch a data classification project to identify critical data for port operations as well as personal data and to protect them accordingly and to map the data flows, especially for personal data and operational data related to vessel, dangerous goods and cargo.

---

\(^{52}\) For now, ports have developed key performance indicators (KPI) to monitor port operations performance, but still very few have implemented key cyber risk reduction indicators (KRIs). See https://www.researchgate.net/publication/283489805_Performance_Indicators_and_Port_Authority_Management

\(^{53}\) As an example, in the US, The Maritime and Port Security Information Sharing & Analysis Center was created in 2015. See https://mpsisao.org/about

\(^{54}\) Compliance with the GDPR is essential for ports, because major attacks against the extraction of personal data have already taken place in the maritime sector (see Table 11).
5.2.4 Asset inventory and management
Security measures regarding ecosystem mapping, including assets of the ports and assets of third-party interacting with the port assets.

- **PS-12**: Use centralised tools for asset inventory and management and ensure that you keep them up-to-date (applications, software platforms, networks, network components, servers, physical devices, OT systems, administration components, etc.).
- **PS-13**: Define a policy regarding authorized devices and software to ensure that only reliable components are introduced to the port network.
- **PS-14**: Use centralised tools to monitor the different assets by adapting them according the specificities and the associated risks (e.g. passive monitoring for OT systems) and detect unauthorized assets.

5.2.5 Cyber resilience (Business continuity and crisis management)
Security measures set up to ensure, in case of any incident, or worst, disaster, the continuity of port operations and recover data.

- **PS-15**: Ensure cyber resilience of port systems by defining objectives and strategic guidelines regarding business continuity and recovery management and set up associated key services and processes (Business Continuity Plan and Disaster Recovery Plan).
- **PS-16**: Define important parameters for port’s business continuity, such as a recovery time objective (RTO), recovery point objective (RPO), maximum tolerable outage (MTO) and minimum business continuity objective (MBCO).
- **PS-17**: Define a crisis management organization by formalising a specific policy and by setting up the associated crisis management process, including all the port stakeholders.
- **PS-18**: Ensure the efficiency of recovery procedures by setting up annual training exercises, making sure that all critical port stakeholders (local authorities, Port Authorities, terminal operators, service providers, etc.) are involved as much as possible, and by formalizing post-exercise reports.

5.3 ORGANISATIONAL PRACTICES
Ports shall define relevant practices and processes regarding IT and OT management, to be followed by all port employees or more specifically by IT and OT teams in their daily operations within the port ecosystem.

5.3.1 Endpoints protection and lifecycle management
Security measures related to the protection of IT end devices such as laptops, desktops, tablets, mobile phones.

- **OP-01**: Define an endpoint protection strategy to monitor port end-devices and to enforce their security by implementing security tools and mechanisms such as antivirus, encryption, mobile device management (MDM) and hardening (disabling of unnecessary services, especially by securing USB ports in all port systems).
- **OP-02**: Implement device and software whitelists and review the list at least annually or in case of a major system change.
- **OP-03**: Define a change management process to introduce any new device into the port systems (acceptance tests, validation steps, etc.).
- **OP-04**: Ensure all employees and contractors return their end-devices at contract termination and define processes for secure end-devices disposal.

---

55 The port of Marseille launched in 2019, into its SmartPort initiatives, a project to map all the port assets: https://lefrenchsmartportinmed.com/les-defis/defi-naval-group
5.3.2 Vulnerabilities management
Security measures to ensure systems are kept up to date and protected from vulnerabilities.

- **OP-05**: Define a vulnerability management process to identify asset vulnerabilities, it can be based on automatic and manual tools such as vulnerability scans.\(^{56}\)
- **OP-06**: Define intelligence processes for cybersecurity in order to be aware of newly disclosed vulnerabilities and take quick compensatory actions (network segregation, service disabling, etc.)
- **OP-07**: Establish tight collaboration of OT and IT departments ensuring that their collaboration with systems business owners, decision-making authorities and other stakeholders is efficient and ensure a homogeneous cybersecurity level for IT and OT.

5.3.3 Human Resource Security
Security measures to ensure good mastery of IT and OT operations and awareness of all employees.

- **OP-08**: Ensure professional references and audits of criminal records of key personnel for IT and OT management (system administrators, developers, etc.) and key personnel appointed in security roles such as CISO or DPO.\(^{57}\)
- **OP-09**: Develop specific and mandatory cybersecurity training courses for some key population dealing daily with IT and OT (system administrators, project managers, developers, security officers, harbour master, etc.).\(^{58}\)
- **OP-10**: Set up a security awareness raising program to address the whole port ecosystem, focusing first on the main threats (e.g. social engineering).\(^{59}\)

5.3.4 Supply chain management
Security measures to understand and secure the relationship with third parties in regards with cybersecurity and ensure legit access to port systems.

- **OP-11**: Strictly control access of third parties to port systems by only granting access on demand, in a specified time window, for a specific purpose, and in a least privileged way.
- **OP-12**: Clearly define all relevant aspects of the partnership with third parties, including security, within the appropriate agreements and contracts, especially for critical systems provided by third-parties (PCS, CCS, security systems, etc.)

5.3.5 Detection and Incident response
Security measures to define processes regarding detection and response of security incidents occurring in the port ecosystem.

- **OP-13**: Identify the risks and threats at all levels of the port to define categories of incidents and the potential impacts by using the results of risk analysis, threat intelligence, previous incident history, discussion with other ports, etc.

---

\(^{56}\) Indeed, every day, most of ports experience multiple vulnerability scans on public IPs from hackers: to thwart these attacks, ports must remediate vulnerabilities before the hackers find them. See [https://pernext.portdebarcelona.cat/en/technology/are-ports-prepared-to-deal-with-threats-from-hackers](https://pernext.portdebarcelona.cat/en/technology/are-ports-prepared-to-deal-with-threats-from-hackers)


\(^{58}\) For example, the Maritime and Port Authority of Singapore have collaborated with the Singapore Shipping Association and Polytechnic to develop a new Maritime Cybersecurity Training course of maritime personnel: [https://smartmaritimenetwork.com/2019/05/16/maritime-cybersecurity-operations-centre-opens-in-singapore](https://smartmaritimenetwork.com/2019/05/16/maritime-cybersecurity-operations-centre-opens-in-singapore)

OP-14: Define a policy and procedures for incident detection and reaction including the description of the roles and responsibilities of each stakeholder of the port or state level (if applicable), as well as the coordination method and communicate this to all relevant parties.

OP-15: Improve and keep these procedures up-to-date by testing them through training exercise, and identification of new feared events.

OP-16: Consider the setup of a Cybersecurity Operations Centre (SOC) including IT and OT environments to support security and cyber incidents. The SOCs of the different stakeholders must collaborate (or can be mutualised) to ensure the detection and reaction of incidents at port level.\(^6\)

OP-17: Define alerting procedures and identify the right contacts for each stakeholder of the port depending on the incident criticality (CISO, port management and board, national authorities, CSIRTs, etc.).

OP-18: Implement procedures for incident reporting and continuous improvement.

5.3.6 Control and auditing
Security measures to control IT and OT compliance to ISSP and to security best practices.

OP-19: Perform regular cybersecurity audits (penetration testing, red team, etc.) to check the application and effectiveness of security measures and assess the level of security of port systems.

OP-20: Perform periodic reviews of network rules, access control privileges and asset configurations.

5.3.7 IT and OT physical protection
Security measures to prevent unauthorized physical access to IT and OT systems.

OP-21: Ensure IT and OT systems hosted in the port are protected following established best practices for safety (fire detection, air-conditioning, etc.) and security (access control, CCTV, etc.)

OP-22: Keep traceability of all maintenance operations done on IT and OT physical systems.

5.4 TECHNICAL MEASURES
Ports shall enforce several technical measures in order to prevent cyber-attacks on ports IT or OT systems, detect and react to any attack and be resilient in case of a major impact from a cyberattack.

5.4.1 Network security
Security measures to avoid unauthorized access to port systems, mitigate the propagation of IT security incidents within systems or subsystems and protect systems from unauthorized access.

TP-01: Define a network segmentation architecture to limit the propagation of attacks within the port systems and avoid direct access from the Internet to very critical port systems such as VTS/VTMIS and security systems.

TP-02: Perform regular network scans to detect unauthorised and malicious networks (WIFI for example) as well as end-devices acting as bridges between two segregated zones (with interfaces in two network zones for example).

TP-03: Define perimetric security, with filtering rules.

\(^6\) For example, the port of Amsterdam established in 2019 a cyber hotline and created the CYREN network (Cyber Resilient North Sea Canal Area) that can be contacted by any companies working in the port. See https://smartmaritimennetwork.com/2019/01/30/new-cyber-programme-for-port-of-amsterdam
5.4.2 Access control
Security measures to ensure legit access to port systems.

- **TP-04**: Set up centralised tools to manage identities and access rights to the port systems. If different tools are set up, due to diversity of the port stakeholders (Port Authorities, terminal operators, local authorities, third-parties, etc.) and their systems, automatic or manual provisioning can be defined.
- **TP-05**: Define an Identity & Access Management (IAM) strategy and its associated processes to manage the lifecycle of identities and their access rights (automatic deactivation of accounts, regular review, least privilege principle and segregation of duties, password guidelines, etc.). This strategy must be, as much as possible, built in common with the stakeholders of the port ecosystem.
- **TP-06**: Forbid as much as possible the use of generic accounts, by enforcing unique and individual accounts in all port systems, especially for sensitive systems (PCS, CCS, TOS, VTS/VTMIS, security systems).
- **TP-07**: Define installation and configuration policy and rules for systems.
- **TP-08**: Implement multi-factor authentication mechanisms for accounts accessing critical applications (especially for PCS, CCS, TOS, VTS/VTMIS) and data (personal data, sensitive operational data such detailed information on vessels, dangerous goods and cargo), and in case of poorly or unprotected environments (external access through Internet for example, third-party access from other corporate networks, etc.).
- **TP-09**: Consider physical access in the access lifecycle (port facilities, port area, buildings, etc.) and define specific measures for remote access.
- **TP-10**: Regularly perform accounts and access right reviews to ensure accesses are still legit, especially for accounts that have access to sensitive data (personal data, sensitive operational data, dangerous goods information, etc.).

5.4.3 Administration and Configuration Management
Security measures to ensure secured administration of IT and OT assets.

- **TP-11**: Define installation and configuration policy and rules and establish security baselines to only install needed services and functionalities and authorise essential equipment for the security and the functioning of port systems.
- **TP-12**: Set up specific accounts only used by administrators to perform administration operations (installation, configuration, maintenance, supervision, etc.).
- **TP-13**: Define Privilege Account Management (PAM) process, security requirements on those accounts and rules to manage their lifecycle. Especially enforce this process for third-parties who oversee administration operations.
- **TP-14**: Set up, as much as possible, dedicated administration networks to create safe zones, in priority for critical systems (especially for VTS/VTMIS, Radio systems, security systems, etc.).

5.4.4 Threat management
Security measures to protect all systems from malware or viruses.

- **TP-15**: Ensure anti-malware, anti-spam and anti-virus is installed and up to date on all port systems, including desktops and servers.

---

61 In 2016, Forrester Research estimated that 80% of security breaches involve privileged credentials
5.4.5 Cloud security
Security measures to protect Cloud environment within ports.

- TP-16: Define a cloud security assessment method to evaluate the impact and the risks of choosing cloud solutions by considering applicable laws and regulations.
- TP-17: Include, as much as possible, security and availability aspects in agreements with cloud security providers.
- TP-18: Try to include, as much as possible, Cloud solutions in the detection and response mechanisms.

5.4.6 Machine-to-machine security
Security measures to secure machine-to-machine exchanges.

- TP-19: Implement mechanisms to secure machine-to-machine exchanges (including EDI messages and API mostly used with external stakeholders, such as shipping companies) and provide mutual authentication, integrity and confidentiality with the port systems such as encryption, PKI or digital certificates, integrity checks, digital signature, timestamping, especially when exchanges are done over the Internet.
- TP-20: Use communication protocols that include a functionality to detect if all or part of a message is an unauthorised repeat of a previous message

5.4.7 Data protection
Security measures to protect data at rest, in transit or in use in port systems.

- TP-21: Implement cryptography procedures and mechanisms to protect confidentiality, authenticity and/or integrity of data in the port systems (at rest, in transit or in use). This measure shall be implemented depending on the data classification done.
- TP-22: Anonymise and secure any direct or indirect personal data processed within the company, e.g. through role-based access control and encryption, having considered all relevant legal requirements.

5.4.8 Update management
Security measures to ensure systems are kept up-to-date.

- TP-23: Define an update management process to ensure that port IT and OT assets are up-to-date, and, if not possible, apply compensatory measures (network segregation, accounts hardening, etc.), especially for legacy systems (OT systems without any possible update, obsolete but critical applications, etc.).
- TP-24: Verify endpoints’ software/firmware authenticity and integrity and ensure tight control over the update.
- TP-25: Verify the source of the update and execute automatic update procedures only if they are based on the risk analysis.

5.4.9 Detection and monitoring
Security measures to ensure IT and OT assets’ health and detect any cyberattack.

- TP-26: Monitor availability of the port systems and devices in real time, where technically feasible, by focusing first on the critical systems and devices such as administration workstations, radio systems and end-devices, VTS/VTMIS, radar systems or security systems and OT end-devices, etc.
- TP-27: Set up logging system to record events related, at least, to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the port systems.
• **TP-28**: Set up log correlating and analysis systems to detect events and contribute to cybersecurity incident detection.

### 5.4.10 Industrial control systems security

Security measures specific to OT systems.

• **TP-29**: Consider OT systems into all the security measures defined in this report to secure as much as possible the industrial control systems and networks. If these cannot be applied, define and implement compensating measures (network segregation, accounts hardening, etc.)

• **TP-30**: Ensure network segmentation between IT and OT systems.

• **TP-31**: When implementing IoT, consider setting up specific security measures.\(^2\)

### 5.4.11 Backup and restore

Security measures to ensure systems recovery in case of incident, linked with the resilience processes defined.

• **TP-32**: Set up backups and ensure they are regularly maintained and tested, especially for most central and critical systems, like Active Directory, PCS, CCS, TOS, etc.

---

6. CONCLUSIONS

As ports undergo their digital transformation, cybersecurity should be viewed not only as a key factor to be considered in terms of keeping pace with the technical evolutions but also as an enabler of further developments and automation. Considering the complexity of both the port landscape in terms of involved stakeholders and communication flows and system interactions, but also in terms of the evolving IT and OT environment, this is by no means an easy or straightforward endeavour.

This report aims to serve as a reference document for stakeholders involved in port cybersecurity. The previous chapters provide an overview of the port landscape, including the policy context, a high-level reference model and a comprehensive asset taxonomy and discuss their cybersecurity dimension by listing the existing threats and security challenges and by describing some key attack scenarios. Finally, the present document provides a list of practical baseline security measures to strengthen cybersecurity in port operations and systems.

Still, people responsible for port cybersecurity, i.e. CISOs, CIOs, IT Managers etc. from Port Authorities and Terminal Operators are encouraged to go beyond the good practices proposed in the present document and address additional topics as well, such as:

- **Awareness raising** about cybersecurity at board and staff level; the former will likely increase the strategic attention paid to cybersecurity risks and result in higher investment and more resources to mitigate them, while the latter is essential in ensuring cybersecurity in day-to-day operations in ports.
- **Improved information sharing** amongst port operators (port authorities, terminal operators etc.) and between port operators and other maritime stakeholders, such as shipping companies. Sharing information on threats, incidents and good practices is key in improving the overall cybersecurity posture of the sector and several proven models, such as ISACs, can be adapted to provide tangible results.
- **Addressing cybersecurity in the supply chain**. While a holistic approach to address this complex issue is not an easy task, several good practices can be adopted or investigated, including cybersecurity certification of critical components, well-defined supplier obligations for the entire lifecycle of products/services (e.g. vulnerability management,patching), specific provisions for supply chain management etc.
- **Integrating interdependencies cybersecurity risks** in the overall cyber risk management process to account for the multiple and complex interconnections of ports with other sectors.
## 7. BIBLIOGRAPHY/REFERENCES

**Sources from European Bodies**


<table>
<thead>
<tr>
<th>Sources from European Member States Bodies</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Sources from Other International Bodies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other sources</td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>N. Polemi, Port Cybersecurity: Securing critical information infrastructures and supply chains, 2017.</td>
</tr>
<tr>
<td>J.M. Constanete, K. Lucenti, S. Deambrosi, Inter-American Development Bank (IDB), International case studies and good practices for implementing Port Community Systems, May 2019. <a href="http://dx.doi.org/10.18235/0001665">http://dx.doi.org/10.18235/0001665</a></td>
</tr>
<tr>
<td>United States Coast Guard (USCG), Maritime Bulk Liquids Transfer Cybersecurity Framework Profile, <a href="https://www.hsdl.org/?abstract&amp;did=797741">https://www.hsdl.org/?abstract&amp;did=797741</a></td>
</tr>
<tr>
<td>P. Chaumette, Cybersécurité dans le domaine maritime, February 2017. <a href="https://humansea.hypotheses.org/771">https://humansea.hypotheses.org/771</a></td>
</tr>
<tr>
<td>D.M. Silgado, Cyber-attacks: a digital threat reality affecting maritime sector, April 2018. <a href="https://commons.wmu.se/cgi/viewcontent.cgi?article=1662&amp;context=all_dissertations">https://commons.wmu.se/cgi/viewcontent.cgi?article=1662&amp;context=all_dissertations</a></td>
</tr>
<tr>
<td>Source</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
</tr>
</tbody>
</table>

**Sources from port websites**

- Port of Tallinn, Smart Port Project. [https://www.portoftallinn.com/smart-port](https://www.portoftallinn.com/smart-port)
### System providers documentation

AP+, Cargo Community Systems, Unir pour optimiser les échanges.  
[www.gyptis.fr/images/mgi/fichiers/Plaquette%20AP.pdf](http://www.gyptis.fr/images/mgi/fichiers/Plaquette%20AP.pdf)

### Press articles


N. Polemi, TechTarget, Port Cybersecurity, July 2018. [https://searchsecurity.techtarget.com/feature/Port-Cybersecurity](https://searchsecurity.techtarget.com/feature/Port-Cybersecurity)


<table>
<thead>
<tr>
<th>Source</th>
<th>Title</th>
<th>Date</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>J. Leyden, The Register</td>
<td>Drug gang hacks into Belgian seaport, cops seize TONNE of smack, June 2013.</td>
<td>June 2013</td>
<td><a href="https://www.theregister.co.uk/2013/06/18/drug_smugglers_using_hackers/">https://www.theregister.co.uk/2013/06/18/drug_smugglers_using_hackers/</a></td>
</tr>
<tr>
<td>N. Newman, Engineering &amp; Technology</td>
<td>Cyber pirates terrorising the high seas, April 2019.</td>
<td>April 2019</td>
<td><a href="https://eandt.theiet.org/content/articles/2019/04/cyber-pirates-terrorising-the-high-seas/">https://eandt.theiet.org/content/articles/2019/04/cyber-pirates-terrorising-the-high-seas/</a></td>
</tr>
</tbody>
</table>
A ANNEX: OVERVIEW OF EU PORT SECTOR

The port sector in the European Union is a complex one. Each port has its own governance and infrastructure model which depends on services delivered, local authorities governance, challenges linked to port geographical situation and national regulations. Ports play a crucial role at different levels for many sectors and have been the successful pioneers in Europe for interconnecting the different types of transport. As a main vehicle for European imports and exports (food, commodities, etc.) with the rest of the world, ports enable also trade and contacts between all European nations. Moreover, ports are important nodes for passengers and vehicles transportation (inter and extra-EU) and play a key role in European fishing activity. Ports ensure also the security and the supply of energy, vital for all EU Member States (fuel, electricity, gas, etc.). Finally, ports have strong impact on society as a source of employment and taking responsibility for pollution prevention.

Additionally, at the European Union level ports are a cornerstone of the development of the Trans-European Transport Network (TEN-T). Moreover, they are at the heart of the maritime ecosystem and as such, key to promote a maritime ecosystem with fair competition, non-discriminatory access to services and efficient use. In May 2013, the European Commission adopted a set of initiatives to increase the competitiveness and the attractiveness of the TEN-T ports: 329 European ports were identified as key ports.

Table 5: Key statistics about ports role in the European Union

<table>
<thead>
<tr>
<th>Key Roles</th>
<th>Key Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port, as a main gateway for the European trade</td>
<td>Almost 90% of the EU’s external freight trade is seaborne, short sea shipping represents one third of intra-EU exchanges in terms of ton-kilometres and 74% of EU trade goes by ship.</td>
</tr>
<tr>
<td>Importance in worldwide trade</td>
<td>Europe counts 3 ports in the top 15 world’s biggest ports: Rotterdam (11th), Hamburg (14th), Antwerp (15th); all three representing 12% of goods handled at a global scale and 20% for EU.</td>
</tr>
<tr>
<td>Key role in energy sector</td>
<td>EU ports have a key role in energy sector: they are energy hubs for conventional and renewable energies and 25% of the ports have more than 50% of their traffic linked to energy commodities.</td>
</tr>
<tr>
<td>Passenger and vehicle transport</td>
<td>Each year, more than 400 million passengers embark and disembark at European ports.</td>
</tr>
<tr>
<td>Social issues</td>
<td>1.5 million workers are employed in European ports.</td>
</tr>
<tr>
<td>Fishing ports</td>
<td>EU is the 4th largest producer worldwide for fish, counting for about 5% of global fisheries. EU trade (i.e. imports and exports) has increased over the past few years, reaching 29.1 billion € in 2014. EU is a net importer of fisheries products and trade between EU countries is very significant and plays an essential role in the EU’s fisheries trade.</td>
</tr>
</tbody>
</table>

---

64 See https://ec.europa.eu/transport/modes/maritime_en
65 See https://ec.europa.eu/transport/modes/maritime/infographics_en
66 See https://ec.europa.eu/transport/modes/maritime/ports/ports_en
68 See https://ec.europa.eu/transport/modes/maritime_en
69 See https://ec.europa.eu/transport/modes/maritime/ports/ports_en
The ranking of biggest European ports is different depending on the activities: the biggest ports related to freight activities are mainly centralised in the North of Europe (Netherlands, Belgium or Germany for the Top 3), while those related to passenger transport activities are mainly situated in the South of Europe or in the Nordics. The EU fishing ports are not so big in comparison with the world fishing ports – only 7 European ports are in the Top 100 biggest fishing ports - and are mainly located in the Nordics.

Table 6: Ranking of the biggest European ports

<table>
<thead>
<tr>
<th>Rank</th>
<th>Port</th>
<th>C*</th>
<th>Volume**</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Rotterdam</td>
<td>🇳🇱</td>
<td>466,360</td>
</tr>
<tr>
<td>2</td>
<td>Antwerp</td>
<td>🇳🇱</td>
<td>208,420</td>
</tr>
<tr>
<td>3</td>
<td>Hambourg</td>
<td>🇩🇪</td>
<td>137,820</td>
</tr>
<tr>
<td>4</td>
<td>Amsterdam</td>
<td>🇳🇱</td>
<td>95,000</td>
</tr>
<tr>
<td>5</td>
<td>Marseille</td>
<td>🇫🇷</td>
<td>81,920</td>
</tr>
<tr>
<td>6</td>
<td>Bremen ports</td>
<td>🇩🇪</td>
<td>73,447</td>
</tr>
<tr>
<td>7</td>
<td>Valencia</td>
<td>🇫🇷</td>
<td>69,600</td>
</tr>
<tr>
<td>8</td>
<td>Le Havre</td>
<td>🇫🇷</td>
<td>68,290</td>
</tr>
<tr>
<td>9</td>
<td>Trieste</td>
<td>🇪🇸</td>
<td>57,180</td>
</tr>
<tr>
<td>10</td>
<td>Constantza</td>
<td>🇬🇷</td>
<td>56,340</td>
</tr>
</tbody>
</table>

*Country ** In thousands of tones

<table>
<thead>
<tr>
<th>Rank</th>
<th>Port</th>
<th>C*</th>
<th>Volume**</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Rotterdam</td>
<td>🇳🇱</td>
<td>14,510</td>
</tr>
<tr>
<td>2</td>
<td>Antwerp</td>
<td>🇳🇱</td>
<td>11,100</td>
</tr>
<tr>
<td>3</td>
<td>Hambourg</td>
<td>🇩🇪</td>
<td>8,730</td>
</tr>
<tr>
<td>4</td>
<td>Bremen ports</td>
<td>🇩🇪</td>
<td>5,470</td>
</tr>
<tr>
<td>5</td>
<td>Valencia</td>
<td>🇪🇸</td>
<td>5,100</td>
</tr>
<tr>
<td>6</td>
<td>Pireus</td>
<td>🇪🇸</td>
<td>4,910</td>
</tr>
<tr>
<td>7</td>
<td>Algeciras</td>
<td>🇪🇸</td>
<td>4,770</td>
</tr>
<tr>
<td>8</td>
<td>Felixstowe</td>
<td>🇬🇧</td>
<td>4,160</td>
</tr>
<tr>
<td>9</td>
<td>Barcelona</td>
<td>🇪🇸</td>
<td>3,420</td>
</tr>
<tr>
<td>10</td>
<td>Marsaxlokk</td>
<td>🇬🇧</td>
<td>3,310</td>
</tr>
</tbody>
</table>

* Country ** In thousands of container TEU

<table>
<thead>
<tr>
<th>Rank</th>
<th>Port</th>
<th>C*</th>
<th>Volume**</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Pireus</td>
<td>🇪🇸</td>
<td>20.9</td>
</tr>
<tr>
<td>2</td>
<td>Dover</td>
<td>🇬🇧</td>
<td>12.9</td>
</tr>
<tr>
<td>3</td>
<td>Paloucia</td>
<td>🇪🇸</td>
<td>11.7</td>
</tr>
<tr>
<td>4</td>
<td>Helsinki</td>
<td>🇫🇮</td>
<td>10.3</td>
</tr>
<tr>
<td>5</td>
<td>Calais</td>
<td>🇫🇷</td>
<td>10.0</td>
</tr>
<tr>
<td>6</td>
<td>Stockholm</td>
<td>🇲🇪</td>
<td>9.2</td>
</tr>
<tr>
<td>7</td>
<td>Helsingborg</td>
<td>🇸🇪</td>
<td>8.3</td>
</tr>
<tr>
<td>8</td>
<td>Helsinger</td>
<td>🇪🇸</td>
<td>8.3</td>
</tr>
<tr>
<td>9</td>
<td>Messine</td>
<td>🇪🇸</td>
<td>8.1</td>
</tr>
<tr>
<td>10</td>
<td>Tallinn</td>
<td>🇪🇪</td>
<td>8.0</td>
</tr>
</tbody>
</table>

* Country ** In billions of passengers

The digital transformation is one of the biggest challenges of the port today. Indeed, ports increasingly rely on IT and OT to be more competitive (through standardization, digitalization and automation), adapt to policies and regulations (especially for administrative procedures or environment protection) and adapt to new maritime assets.

Table 7: Example of stakes leading to digital transformation for ports

<table>
<thead>
<tr>
<th>Stake</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated logistic chain development</td>
<td>In order to boost its attractiveness and performance, ports have to offer to their clients the most efficient global and integrated logistic chain: they provide value-added services that includes integrated services. For example, some ports now offer the service of filling in customs declarations on behalf of maritime companies. The port systems become then a central point for data exchange for all port ecosystem stakeholders.</td>
</tr>
<tr>
<td>Environmental stakes</td>
<td>In April 2018, at the 22nd session of Marine Environment Protection Committee, IMO adopted a strategy to reduce pollution such as gas emission in the maritime sector. In parallel, ESPO presented its annual Environmental Report for 2018 at the Greenport Congress, including performance benchmark indicators and the Top 10 Environmental priorities of the ports. New technologies will help ports to reach their objectives in terms of sustainability.</td>
</tr>
<tr>
<td>Digitalization and standardisation of administrative procedures</td>
<td>Administrative procedures related to the maritime ecosystem are often complex and time-consuming. Several initiatives have been launched to digitalise these procedures and set up modern electronic data systems. In a 2009 European Commission Communication, a true “European maritime transport space without barriers” is established to improve electronic transmission. The notion of “single window” has also developed to streamline the access to the various ICT systems from a unique portal for the whole port community. Other “single window” systems are developed by EMSA at National (NSW) and EU level (EMSW).</td>
</tr>
<tr>
<td>New generation of vessels</td>
<td>Two stakes are related with the construction of new generation of vessels and will impact strongly the ports: the vessels are built to be bigger and more and more connected. The new generation of vessels are built to be more connected to reduce cost and security issues. The ship builders are already designing the autonomous ships that could go to sea with strong impacts on ports IT environments.</td>
</tr>
</tbody>
</table>

Ports must be increasingly innovative and find ways to address those stakes while keeping their operations safe and secured. This is one of the reasons why the concept of “Smart Port” has emerged. Through this concept, we can find different types of innovations and initiatives, detailed in Table 8: Detailed innovations that ports set up linked with “Smart Port” concept: IoT, blockchain, cloud, automation, artificial intelligence and many more. Those innovations bring also new stakes in terms of cybersecurity as they place IT and OT at heart of ports operations.

72 For example, in the port of Rotterdam, the customs declarations can be filled in through the Port Community System: https://www.portofrotterdam.com/en/doing-business/services/service-range/port-customs
74 See Modernisation of Port Authorities’ Management Information Systems (PMIS), Jonas Mendes Constante – Fundación Valenciaport, Martina Grzancic – Luka Kopler
77 See SmartPort definition: http://parisinnovationreview.com/articles-en/what-is-a-smart-port
78 See Port Digitalization with Open Data: Challenges, Opportunities, and Integrations: https://www.researchgate.net/publication/321853773_Digital_transformation_in_maritime_ports_analysis_and_a_game_theoretic_framework
### Table 8: Detailed innovations that ports set up linked with “Smart Port” concept

<table>
<thead>
<tr>
<th>Innovations</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internet of Things (IoT)</strong></td>
<td>Various ports are studying or launching an IoT project to improve their competitiveness and their performance and monitor their infrastructure to prevent security or safety incidents. Applied to maritime traffic surveillance, infrastructure management and terminal operations on goods or passengers, an IoT platform could monitor the port environment and operations, collect data to optimize processes and improve the decision-making process. This would be possible through the implementation of sensors and RFID technology on port assets. More specifically, the port of Rotterdam has launched his own IoT platform by implementing different sensors on buoys, walls and quays to allow port actors to identify the best timing and location for a ship to dock.</td>
</tr>
<tr>
<td><strong>Cloud</strong></td>
<td>In order to coordinate all the stakeholders of their ecosystem and enable an efficient and real-time exchange of data in a centralised way, some ports have recently launched Cloud projects to improved operations efficiency and develop “Port Single Window” systems, central systems to manage all data exchange related to the port operations and mandatory declarations. For example, SOGET, a public-private partnership between the Port Community of Le Havre, Port of Le Havre Authority and French Customs, in charge of developing the e-Maritime Port Single Window, has developed a partnership with a cloud provider to base its solution on Cloud technology.</td>
</tr>
<tr>
<td><strong>Big Data</strong></td>
<td>The entire port ecosystem manages everyday a vast amount of data for different objectives (data related to monitor the movements of ships and the movements of cargo or container, to manage the port infrastructure, etc.). Today, in most ports, the potential of the data is not yet fully exploited because the data are often used in silos without correlating them. Some ports are currently launching Big Data projects to improve port operations, processes, security and safety. For example, collecting and correlating information on ship positions arriving, leaving or staying in ports and weather can enable to prevent accidents. For example, the port of Valencia has recently launched a Big data project to improve the efficiency of terminal logistics to optimize the operations and set up an advanced dashboard.</td>
</tr>
<tr>
<td><strong>Blockchain</strong></td>
<td>Seaborne trade is very inclined to malicious activities such as organized crime: a real need exists today in port ecosystem for data trust and privacy, especially for container management, that it is accentuated by the complex panorama of stakeholders included in the logistic chain of a port. Indeed, to transport a container, it can involve more than 30 different parties, with an average of 200 interactions between them. The application of blockchain on port operations and processes seems to be an excellent way for ports to bring trust and privacy with smart contracts. Indeed, the port of Antwerp has recently collaborated with a blockchain start-up to develop a solution adapted to the port processes concerning certificates (for instance, phytosanitary certificates).</td>
</tr>
<tr>
<td><strong>Automation</strong></td>
<td>One of the key success factors for the increase of the competitiveness, the efficiency and the performance of a port is to automate as much as possible port operations and processes. Numerous innovations are developed today with ports to automate these processes at all levels. For example, ports are deploying aircraft and aquatics drones or also automated gates, studies are being carried out to make cranes autonomous, etc. For instance, the ports of Rotterdam and Amsterdam have authorized aerial and marine drones in their areas to improve the port operations (maintenance inspections, management of incidents and emergencies, etc.).</td>
</tr>
<tr>
<td><strong>Prediction and analytics through artificial intelligence</strong></td>
<td>In parallel of projects of automation, Big Data, IoT, etc., artificial intelligence can bring an in-depth analysis of the data related to all port operations and processes and deploy a predictive model of the behaviour of port operations. For example, the artificial intelligence can give to the terminal operators a dynamic forecast of the port conditions and environment, such as real ship arrival time or saturation of access routes. The port of Antwerp has recently launched a data science project to better optimize the operational chain, anticipate bottlenecks and improve decision-making process.</td>
</tr>
</tbody>
</table>

---

82 See https://www.patersonsimsons.com/wp-content/uploads/2018/06/TMS_SmartPort_InsightBee_Report-to-
84 See https://www.i-scoop.eu/blockchain-smart-port-project-case-container-release-port-antwerp
87 See https://ipiernet.portdebarcelona.cat/en/technology/artificial-intelligence-ports-are-beginning-to-take-up-positions
### C ANNEX: CATEGORIES OF PORT STAKEHOLDERS

Table 9: Categories of port stakeholders

<table>
<thead>
<tr>
<th>Categories</th>
<th>Sub-Categories</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Authority</td>
<td>The Port Authority, a governmental or almost governmental public authority, sitting at the heart of the interactions between all stakeholders, in collaboration with other local and national authorities, is responsible of maintaining and developing the port infrastructure and the transport infrastructure, ensuring the global safety and security of port and ship operations through the harbour master. Moreover, the Port Authority oversees some controls and inspections in respect with national, European and international legislations.</td>
<td></td>
</tr>
<tr>
<td>Port Terminal Operators</td>
<td>Terminal operators, usually private companies, are responsible for maintaining security and safety on the land they rent from the Port Authority and managing the services related to terminal operations (loading and unloading cargo or passengers for instance).</td>
<td></td>
</tr>
<tr>
<td>Vessels related stakeholders</td>
<td>Shipowners and crew</td>
<td>The shipowner is in charge of equipping and exploiting a commercial vessel, hiring licensed crew and captains to operate the ship.</td>
</tr>
<tr>
<td></td>
<td>Flag state</td>
<td>The flag state of a commercial vessel is the jurisdiction under whose laws the vessel is registered: the flag state enforced regulations such as inspection, certification, and security requirements. Each vessel operates and navigates under the law of its flag state that list and enforce international conventions (IMO conventions notably).</td>
</tr>
<tr>
<td></td>
<td>Ship insurance</td>
<td>Ship insurance covers the loss or damage of ships, cargo, terminals, and any transport by which the property is transferred, acquired, or held between the points of origin and the destination.</td>
</tr>
<tr>
<td>Delivery chain stakeholders</td>
<td>Shipping and maritime freight companies</td>
<td>These private companies are in charge of transferring and forwarding freight from a place to another, by bookings services for all kind of transport (maritime transport, railways, etc.).</td>
</tr>
<tr>
<td></td>
<td>Ferries and cruise lines</td>
<td>These private companies oversee offering to passengers’ transport services through ferries and cruise.</td>
</tr>
<tr>
<td></td>
<td>Fisheries</td>
<td>According to the Food and Agriculture Organization of the United Nations, a fishery is typically defined in terms of the “people involved, species or type of fish, area of water or seabed, method of fishing, class of boats, and purpose of the activities or a combination of the foregoing features”.</td>
</tr>
<tr>
<td></td>
<td>Hinterland liaisons</td>
<td>This category relates to all stakeholders, private as public, interacting in the multi-modal ecosystem of the port: waterways, roads, railways, etc.</td>
</tr>
<tr>
<td></td>
<td>Freight sender and consignee</td>
<td>The sender is the person, company or organisation, at the origin of the forwarding of a good or other item which can be sent by sea.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The consignee is the receiver of this good, also a person, a company or an organisation.</td>
</tr>
<tr>
<td></td>
<td>Maritime agent</td>
<td>Also called ship agent, the maritime agent acts as a representative of the shipowner to fulfil the requirements for each port the ship visits.</td>
</tr>
<tr>
<td>Service providers</td>
<td>Ship services providers</td>
<td>A ship can book different services to the port. For some of these services, the port delegates these services to external companies (e.g. refuelling).</td>
</tr>
<tr>
<td></td>
<td>Dockers</td>
<td>The dockers are employed by private companies – which could be terminal operators – to realise the terminal operations (e.g. loading and unloading vessel cargo).</td>
</tr>
</tbody>
</table>
## Security providers
To ensure security in ports, private companies operate and maintain security systems in the port (such as CCTV).

## Infrastructure providers
A port can contract private companies to operate in the port to ensure the installation of port infrastructure and its maintenance.

## Ship repair services
Shipping companies or shipowners can book ship repair services to the port for damage cases of all kinds, delivered by different actors depending on their expertise (propulsion systems, governors, etc.).

## ICT integrators
To support the port processes and operations, ports use daily Information and Communication Technology (ICT) systems which are, for most of them, set up, operated and maintained by private specialised companies in IT and Communications development.

## Classification societies
As a non-governmental organisation, classification societies set standards for the construction and operation of ships and offshore structures and certify that the construction of a ship complies with those standards by delivering a certificate.

## Other entities
The port ecosystem includes many secondary actors, the most important of which are as follows:
- Banks: As in any business, ports deliver different services that they invoice to shipping companies and other stakeholders. Banks are therefore a key factor in these services.
- Organisations and associations, created for different objectives and at different levels. For instance, the ESPO (European Sea Ports Organisations) is acting as the main interface between European seaports and European institutions, IAPH (International association of Ports and Harbours) is the global trade association for seaports worldwide, the IPCSA (International Port Community System Association, etc).
- Innovation, Research and Education stakeholders: the port ecosystem is composed by different actors acting strongly in favour of innovation (such as start-accelerators, with, for example PortXL, alliances for developing Smart Port), research (research and expertise centres) and education (universities).

## Other commercial providers
- **Customs**
  The customs authorities are responsible of the administration and the application of national and international customs law through the collection of duties and taxes, in particular for importation, exportation, movement or storage of goods in ports.

- **Fishery Control**
  The fishery control authorities are in charge to ensure the fishing of good quality and sustainable seafood by defining controls and requirements that the fishing industry must follow. For instance, they control the permit for a vessel to fish, the origin of the fish catches, etc.

- **Coast Guards**
  Coast Guards are maritime organizations in charge of ensuring navigation safety and security and enforcing the law on the maritime territory under the responsibility of the country.

- **Border Control**
  The border control authorities are responsible of taking measures to monitor the state borders and to regulate the movement of people, animals and goods. In the EU, with Schengen agreement, the crews and passengers are controlled only once when they come from a non-EU country.

- **Port State Control**
  The Port State Control is responsible of making inspections of foreign ships (with a flag state different from the port) in ports to verify the compliance of the ships with international and national regulations. The Port State Control can take actions against non-compliant ships (sanctions, etc.).

- **Civil Security, police and rescue at sea**
  The civil security and police authorities are responsible of law enforcement and of deploying measures to fight against criminals (terrorism, organized crime, etc.). Each port has its own local civil security and police. According to local and national specificities, they can also oversee rescue at sea to assist people and vessels in case of distress situations.

- **Prevention of Pollution**
  The prevention of pollution authorities are responsible of ensuring that national and international regulations are applied in the port ecosystem (management of ship waste, etc.).
| **Cities** | At local level, the cities are strongly involved in the development and the operations of ports: investment in port infrastructure, in maritime tourism, planification of road construction, financing university research, etc. The cities are a major stakeholder involved in the construction of each port strategy. |
| **International bodies** | At international level, they are also different bodies involved in port ecosystem, for instance: IMO (International Maritime Organization), WCO (World Customs Organization), IMB (International Maritime Bureau, a specialised division of the International Chamber of Commerce acting against all types of maritime crime and malpractice), CIMSEC (Centre for International Maritime Security), etc. |
| **EU Agencies** | Numerous EU agencies are involved in the port ecosystem, interacting mainly with the local and national authorities detailed above, for instance: EMSA (European Maritime Safety Agency), EFCA (European Fisheries Control Agency), FRONTEX (European Border and Coast Guard Agency), EUROPOL (European Police Office), ENISA (European Union Agency for Network and Information Security Agency), etc. |
| **Maritime administrations and national authorities and bodies** | At national level, we find the same types of authorities as at the international and European level, considering the specificities of each Member State: maritime administrations\(^{88}\), Ministry of Transport, etc. |

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe’s citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe’s critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolacu Plastira
700 13 Vassiliki Vouton, Heraklion, Greece

enisa.europa.eu