Grant Agreement Number: ***833389***

Project acronym: Cyber-MAR

Project full title: Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain

D8.1. Guidelines for Cybersecurity Training Programme across EU (Intermediate)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389. The content of this document reflects only the authors' view and the European Commission is not responsible for any use that may be made of the information it contains.

Document Identification	
Status	Final
Version	1.00
Related WP	WP8
Related Deliverable(s)	D8.2, D8.3, D8.4
Lead Participant	ATOS
Contributors	ALL
Due Date	Monday, 31 August 2020
Submission Date	01/09/2020
Document Reference	D8.1
Dissemination Level	P
Document Type:	R
Lead Author	Gustavo González-Granadillo
Reviewers	George Baroutas, ICCS
	Kemedi Moara-Nkwe, UoP

Legal Disclaimer

Document Information

List of Contributors	
Name Surname	**Beneficiary short name**
Gustavo Gonzalez-Granadillo, and José Crespo	ATOS
George Baroutas	ICCS
Thierry Maur	NG
Anna-Mari Heikkila, Sami Noponen, and Jarkko Kuusijarvi	VTT
Michael Kotras	PCT
Jean-Baptiste Rouault, and Mathieu Leturcq	DIATEAM
Pablo Gimenez, and Mercedes de Juan	VPF
Fabio Ballini, and Monica Canepa	WMU
Beatriz Bazzica, and Carmen Giordano	FAIMM
Kimberly Tam, and Kevin Jones	UoP
Vasiliki Palla	SEAB
Euripides Sakellariou, and Panagiotis Athanasopoulos	PEARL
Luis Sousa, Kamban Parasuraman, Barbara Chang, Julia Mattes, and Bernhard Reinhardt	AIR

Document History			
Version	**Date**	**Change editors**	**Changes**
0.1	17/03/2020	Gustavo Gonzalez	ToC
0.2	25/03/2020	Gustavo Gonzalez	Refined ToC + role assignment
0.3	31/03/2020	Gustavo Gonzalez	Stakeholder Analysis (draft)
0.4	10/04/2020	Gustavo Gonzalez	Stakeholder Analysis refinement (based on comments from ICCS and SEAB)
0.5	24/04/2020	Gustavo Gonzalez	PESTEL Analysis (draft)
0.6	07/05/2020	Gustavo Gonzalez	PESTEL Analysis refinement
0.7	18/05/2020	Gustavo Gonzalez	Cyber-MAR Ecosystem (draft)
0.8	28/05/2020	Gustavo Gonzalez	Cyber-MAR Ecosystem (refinement) adding contributions from all partners
0.9	15/06/2020	Gustavo Gonzalez	Main findings + Introduction and conclusions
0.10	29/06/2020	Gustavo Gonzalez	Document refinement
0.11	06/07/2020	Gustavo Gonzalez	Additional information to Cyber-MAR Ecosystem

Document History			
Version	**Date**	**Change editors**	**Changes**
0.12	21/07/2020	Gustavo Gonzalez	Final refinements before quality assurance review
0.13	10/08/2020	Gustavo Gonzalez	Implementation of comments from ICCS
0.14	24/08/2020	Gustavo Gonzalez	Implementation of comments from UoP
1.0			Final version to be submitted

Quality Control		
Role	**Who (Partner short name)**	**Approval Date**
Deliverable leader	ATOS	31/07/2020
Quality manager	ICCS, UoP	24/08/2020
Project Coordinator	ICCS	09/08/2020

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
cPPP	contractual Public-Private Partnership
CEF	Connecting Europe Facility
CERT	Computer Emergency Response Team
CO_2	Carbon Dioxide
CSIRT	Computer Security Incident Response Team
DoA	Description of Action
EC	European Commission
ECSO	European Cyber Security Organisation
EFCA	European Fisheries Control Agency
EMSS	European Maritime Security Strategy
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
FAL	Facilitation of International Maritime Traffic
GCI	Global Cybersecurity Index
GDP	Gross domestic product
GDPR	General Data Protection Regulation
GHG	GreenHouse Gas
HICP	Harmonised Index of Consumer Prices
ICS	Industrial Control Systems
ICT	Information and Communications Technology
ILO	International Labour Organization
ISM	International Safety Management
ISO	International Organization for Standardisation
ISPS	International Ships and Port Facilities Security
IT	Information Technology
IMO	International Maritime Organization
MACN	Maritime Anti-Corruption Network
MSC	Maritime Security Committee
NCSS	National Cyber Security Strategy
NOx	Nitrogen Oxides

Abbreviation / acronym	Description
OT	Operational Technology
PII	Personal Identifiable Information
R&D	Research and Development
SOLAS	Safety of Life at Sea
SOC	Security Operation Centre
SOx	Sulphur Oxides
SWOT	Strengths, Weaknesses, Opportunities, Threats (Tool)
UftM	Union for the Mediterranean
UNCTAD	United Nations Conference on Trade and Development
VftF	Vessels for the Future
WP	Work Package

Executive Summary

This document provides an analysis on the most relevant external factors that impact the cybersecurity and maritime sectors in Europe. The first part of the analysis focuses on the Political, Economic, Social, Technological, Environmental and Legal (PESTEL) factors affecting directly or indirectly the cybersecurity and maritime domains. In addition, a stakeholder analysis is presented where three main stakeholder groups are identified: cybersecurity, shipping, and port. For each of them, internal and external key stakeholders are identified including consortium partners and external organizations (e.g., clients, providers, competitors, etc.) in the cybersecurity and maritime domain. Furthermore, an analysis of the current cybersecurity and maritime situation in Europe, is presented in the deliverable by focusing on the national strategies and plans developed by several European countries. The Cyber-MAR ecosystem analysis aims to identifying aspects related to the regulatory framework, initiatives, challenges and existing gaps in both, the cybersecurity and the maritime industries.

As a result, although the PESTEL analysis indicates that most studied factors fall into the Positive (P) or Very Positive (+P) categories, factors such as global political conflicts, the EU current economic situation, the cybersecurity maturity in the EU, climate change, and environmental challenges (COVID-19) are among the potential negative factors to be considered as threats in Cyber-MAR. In addition, the stakeholder analysis performed in Cyber-MAR positions key stakeholders into four main categories: key players, context setters, crowd and subjects, for which strategies are proposed to manage and meet their needs. Finally, among the challenges identified in the Cyber-MAR ecosystem analysis, the lack of cybersecurity awareness, lack of qualified personnel and poor bilateral/multilateral collaboration appear to be common in most studied countries. Several initiatives have been identified in both sectors, with the National Cybersecurity Strategy as one of the major actions taken by all studied countries.

D8.1 is the initial version of the Cyber-MAR market watch and should be considered as a starting point to define strategies for exploitation and commercialization routes. This document will be continuously updated and complemented with a final version (D8.2) to be released at M36 of the project including actions and recommendations to reduce the supply deficient of cybersecurity training in the maritime domain within the EU.

1. Introduction

1.1 Purpose of the document

This document is created with the objective of providing information about external factors (e.g., regulations, policies, market watch) on the state of play of the maritime cybersecurity industry in Europe, as well as in member states, and allows to assess what challenges are posed and what progress is taking place.

The main purpose of this document is to increase awareness in terms of the limitations and existing gaps in the maritime cybersecurity area in Europe as well as on the current initiatives performed in both sectors and the actions to be taken to improve cybersecurity protection in the maritime critical infrastructure. The on-going assessment of the challenges and barriers that exist in the domain will be focused on the impacts achieved in terms of cyber range capacities and soft skill development through the different pilots and training activities conducted in WP5 and WP6 respectively. As a result, two versions of the document entitled "Guidelines for Cybersecurity Training Programme across EU" is expected to be produced within the three years of the project.

The first version of this document (i.e., D8.1 due at M12) will focus on a diagnostic analysis of the current situation in both sectors, having a particular interest in identifying challenges and gaps that would be potential barriers in the accomplishments of the tasks planned in the project. The final version (i.e., D8.2 due at M36) will refine the analysis and provide guidelines and recommendations supporting the cybersecurity cPPP, including actions to reduce the supply deficient in the EU.

As stated in the DoA [DOA19], a socio-economic aspect will be considered in the policy paper to reinforce adoption for job creation as skilled "cybersecurity experts" and increase welfare through adoption of the Cyber-MAR solutions and services.

1.2 Intended readership

This deliverable will be publicly available; therefore, it is intended to be used by all consortium members and in general, any kind of person interested in the current landscape of the maritime and cybersecurity industries. Key stakeholders from private and public sectors might be interested in the challenges and gaps to which the cybersecurity and maritime domains are exposed to and could benefit from the guidelines and recommendations obtained out of the environmental analysis presented.

1.3 Document structure

This deliverable is structured as follows:

- Section 2 defines the exploitation objectives and the methodology used to accomplish them.
- Section 3 presents the Cyber-MAR environment analysis, focusing on the Political, Economic, Social, Technological, Environmental, and Legal factors affecting the activities of the project.
- Section 4 presents a stakeholder's analysis and focuses on the identification, understanding and mapping of key stakeholders to the Cyber-MAR project.
- Section 5 analyses the Cybersecurity and Maritime ecosystem in Europe, focusing on eight European countries i.e., Finland, France, Germany, Greece, Italy, Spain, Sweden, and the U.K.
- Section 6 provides a global picture on the challenges, initiatives, and gaps identified on the maritime cybersecurity sector in the EU and presents preliminary recommendations.
- Section 7 concludes the document.

2. Exploitation Objectives and Methodology

Considering the following exploitation objectives for Cyber-MAR:

- Making the results and benefits of the developed solutions attractive and known to all key stakeholders.
- Ensuring the solutions developed are both validated and viable for longer-term exploitation.
- Developing an impact plan focusing on the potential for further exploitation of the innovations towards the end and after the end of the project.
- Ensuring that the potential exploiters of project results are made aware of the support networks, tools and grants available to them within the EU and given details on how to access them.

The exploitation activities have been designed to guide technology providers into refining and accomplishing their individual exploitation plans and increasing the chances to reach to a wider market. The methodology to be used for T8.1 (Market watch and policy activities) will focus on two main phases: (i) the analytical phase, comprising analysis and planning activities to be execute during the first half of the project in order to gather information about internal and external factors that would affect (directly or indirectly) all activities performed during the project, and (ii) the strategic phase, comprising decision, action and assessment activities to identify gaps and barriers affecting the maritime cybersecurity industry and provide guidelines for cybersecurity training and recommendations to cope with the identified deficiencies. Figure 1 depicts the main the methodology to be followed for each task of WP8.

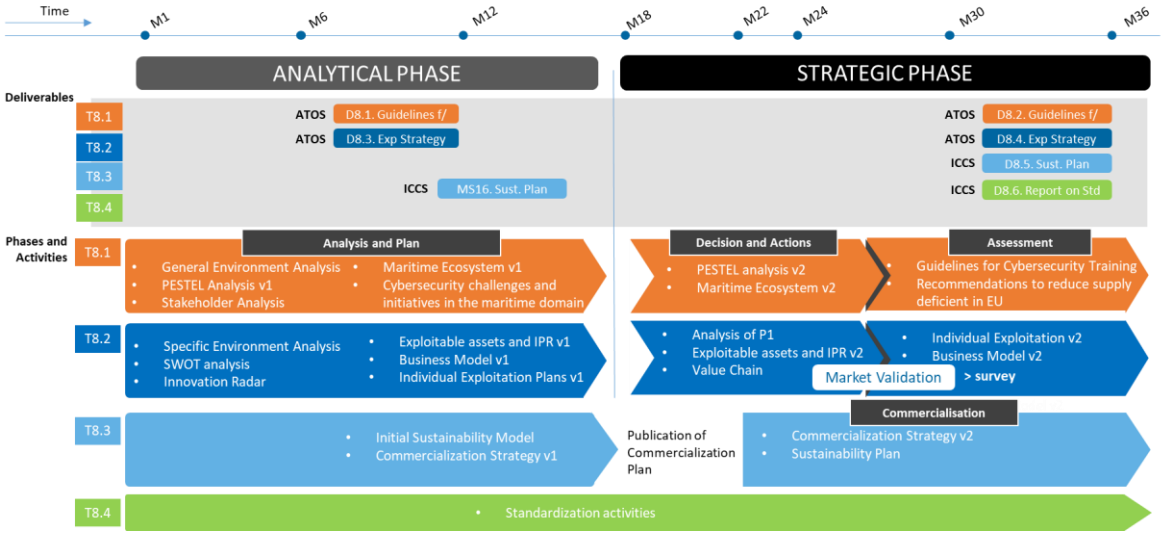


Figure 1. Cyber-MAR Exploitation Methodology

Having a close look at T8.1, Figure 1, shows that during the first half of the project (M1-M18) this task will focus on a general environment analysis of the current cybersecurity and maritime situation in Europe and will provide a first version of a PESTEL analysis, a stakeholder analysis and an initial version of the Cyber-MAR ecosystem, focusing on existing challenges and initiatives in this domain. The analysis will lead to the identification of gaps and barriers that will be complemented within the second half of the project (M19-M36) with a refined version of the PESTEL analysis and the Cyber-MAR ecosystem, as well as with guidelines and recommendations to minimize the identified gaps and barriers.

3. Cyber-MAR Environment Analysis

One of the key phases of the Cyber-MAR exploitation strategy is the analysis of external factors that could directly or indirectly affect the development of the project' assets, as well as their introduction into the market. Political, Economic, Social, Technological, Environmental and Legal factors are analysed within the context of the maritime cybersecurity industry. Each factor has been assigned a code (e.g., Po1, Ec3, So4) and an assessment level that identifies if the factor provides a very positive (+P), positive (P), neutral (X), negative (N) or very negative (-N) effect over the project's activities.

A special mention should be made on the Corona Virus (COVID-19) outbreak situation, that has affected businesses and people all over the world with devastating consequences in all areas. The COVID-19 crisis escalated to unprecedented levels in Europe since March 2020, with a severe impact on health, people and economy. It had a major impact on global shipping, affecting all shipping sectors from passenger ships to container ships and oil tankers [EMS20].

The global crisis and social distancing measures are preventing technicians flying out to ships and rigs to upgrade and service critical operating systems, resulting in established security protocols being circumvented, leaving businesses open to attack [NAU20]. The proliferation of spam emails, phishing campaigns, fraudulent calls, fake online products/services, malware, and ransomware are among the most common attacks detected during the second trimester of 2020 [PIP20].

The current situation has drastically changed customers' behaviours and habits, as well as the way of doing business. Cybersecurity has been a major aspect to highlight, with half of the world being connected remotely to their companies, schools and social life. Remote working and e-commerce have significantly increased the importance of securing the digitalised trade. In addition, decreasing volume as well as tendency to more localised value chains instead of global based supply chains are starting to be discussed.

While many companies are challenged to survive in the short-term, the crisis also presents opportunities; bold companies that invest ambitiously and timely in their online business are likely to emerge as market leaders [DEL20]. Table 1 summarizes the PESTEL analysis performed for the Cyber-MAR project.

Table 1. Cyber-MAR PESTEL Analysis Summary

PESTEL	Cod	Analysis Points	P+	P	X	N	N+
Political	Po1	Protectionism			X		
	Po2	EU political conditions		X			
	Po3	Global political conflicts					X
	Po4	Globalization's impact			X		
	Po5	Anti-corruption initiatives		X			
	Po6	Other political factors				X	
Economic	Ec1	Increasing competitiveness on ports		X			
	Ec2	Investment in innovative solutions	X				
	Ec3	Blue economy			X		
	Ec4	EU current economic situation					X
	Ec5	Business opportunities in the cybersecurity and maritime sectors		X			
	Ec6	Direct economic incentives to improve cybersecurity in the maritime sector	X				
	So1	Cybersecurity and Maritime stakeholders' relationship		X			

Social	So2	Awareness on maritime cybersecurity		X			
	So3	Education and skills	X				
	So4	Consumer habits		X			
Technological	Te1	Making use of digitalization		X			
	Te2	Cybersecurity maturity in the EU				X	
	Te3	Rapid advances in technology		X			
	Te4	Convergence of IT and OT	X				
	Te5	Vulnerabilities in Industrial systems		X			
	Te6	Cyber incident handling process in the maritime domain			X		
Environmental	En1	Vessels for the future (VftF)	X				
	En2	Environmental challenges and issues				X	
	En3	Environmental protection initiatives		X			
	En4	Climate change				X	
Legal	Le1	International Context			X		
	Le2	EU regulations		X			
	Le3	EU national strategies	X				
	Le4	Data Protection (GDPR)		X			
	Le5	Brexit and the maritime industry				X	

3.1 Political Analysis

Cyber-attacks are a growing threat spreading to all kinds of industry relying on ICT systems. Recent events prove that cyber-attacks have a significant impact on critical infrastructures. Their consequences for the EU Member States' governments and social wellbeing are huge and go beyond monetary values, threatening the safety of an organization, a city and even a whole nation. Thus, it is vital to ensure ICT robustness against cyber threats at national and European level [MCS11].

Cyber security in the maritime domain requires a well establishment of policies, reforms and regulations that influence the infrastructure and operations of port facilities including shipping services. Political factors play a significant role in the definition of the aforementioned aspects [FFU20]. The analysis of the political factors in Cyber-MAR include the following:

- **Protectionism:** this term refers to the restriction of trade among countries by imposing taxes on imported products, pushing consumers to privilege domestic over imported products. The current spate of uncertainties and speculations surrounding President Trump's plans to impose taxes on international trade, and its impact on international shipping is an example of this factor [MAI20]. The Cyber-MAR solution could be greatly affected by any kind of protectionism implemented in countries where the key target customers operate. This factor can be positively used to protect Cyber-MAR solutions in the EU from having to pay additional taxes but can negatively affect the commercialization of the Cyber-MAR assets outside the EU.

- **EU Political Conditions:** By 2020, all 27 member states of the European Union are considered as totally free electoral democracy [ABR18]. Each member is party to the founding treaties of the union and thus shares in the privileges and obligations of membership. All EU member states have agreed to share sovereignty through the institutions of the European Union in some aspects of government. In addition, EU financial unity intensifies political alignments among all member states, which can be a

positive factor to be considered by the Cyber-MAR project. However, the antidemocratic influence of countries outside the EU (e.g., China, Russia), have expanded all over the world, taking advantage of the domestic problems and policy priorities of the United States and other democratic powers [ABR18].

- **Global Political Conflicts:** The tensions between China, Philippines and Vietnam about the South China Sea dispute has increased China's military activity and conducted a series of naval manoeuvres in the area [GCT20]. In addition, the U.S. has stepped up its military activity and naval presence in the region, which includes six freedom of navigation operations (FONOPs), causing a tension increase between China and USA [Bee20]. Furthermore, the Iranian – American confrontation intensifies military tension between Iran and the USA in the Persian Gulf region. Such events could eventually affect negatively the trade deals with partners around the world and, ultimately, obstruct shipping [BIS19]. Additionally, State-sponsored cyberattacks/espionage have enormously increased, as they are highly rewarded with relatively low cost/low risk to carry out [FSEC20]. The impact of this factor can be considered as very negative for the Cyber-MAR project.

- **Globalization's Impact:** Living in a globalized world, where raw materials produced in one country are shipped to another country (and even another continent) before being commercialized in the market, is a normal activity that many organizations are exposed to in their every day's operations. Cotton grown in the U.S. is sent to Africa and then to the Asia for further processing, which substantially reduces overhead costs before returning the finished products back to Europe and North America for retail sales [MAI20]. The shipping industry has been a key element in fostering trade, and both the cybersecurity and maritime industries perfectly adapted themselves with technologies, national registries, and labour resources to fit to the demands of globalization. The impact on human resources has been very positive, with specific international qualification standards and crew training protocols in place, modern technology is operated by international human talent [MIS18]. Political relationships and alliances might impact positively on the shipping of goods and merchandises. They may also play a negative effect in trades and negotiations while doing business. Political conflicts (e.g., civil unrest in Africa) as well as other global incidents (e.g., COVID-19) may disrupt the value chain, forcing diversion of goods for processing elsewhere, or even processing at the source, minimizing the need for shipping. Political activism that exposes child or slave labour may have a similar impact, forcing processing at sources in closer proximity and potentially eliminating the need for ocean shipping [MAI20]. The impact of this factor can be considered as neutral for the Cyber-MAR project.

- **Anti-corruption Initiatives:** Although in today's world, most companies have an internal defence against unethical practices, corruption continue to exist. From false certificates and checklists to briberies regarding safety inspections, corruption is one of the biggest impediments to achieving the sustainable development of shipping industry [SAF18]. In addition, bureaucracy and interference in the shipping industry by the government is an aspect that could affect negatively the deployment and usage of the Cyber-MAR solutions. However, many initiatives have been developed to fight against corruption all over the world. Examples of these initiatives are the international anti-

corruption day[1], the Maritime Anti-Corruption Network (MACN[2]), and sustainability safety4sea awards[3] are created to spread awareness and make the industry safer, more profitable and sustainable. The impact of this factor can be considered as positive to the Cyber-MAR project.

- **Other Political Factors:** Although economic aspects (e.g., cost and time) are considered as key important aspects in the cybersecurity and maritime industry, political aspects are often neglected. Customers tend to privilege low-cost options and/or quick delivery, depending on the type of product and urgency required to be transported. In most of the cases, customers do not give importance to threats in the delivery, bottlenecks in ports, trade union activism, civil disturbances and any other kind of incident that could directly or indirectly affect the shipment of cargo [MAI20]. These political factors can distort the maritime industry and modify the choice of transportation, which could be considered as a negative impact for the Cyber-MAR project.

3.2 Economic Analysis

Economic factors affecting the Cyber-MAR project cover both macro-environment indicators (e.g., growth rate, income, inflation, interest, etc.); and micro-environment indicators (e.g., competitors' impact, investments, etc.). This section analysis the following economic aspects:

- **Increasing competitiveness on ports:** Europe is one of the leading maritime centres in the world, with 400 million passengers traveling by sea in the EU; three out of four parts of EU's external trade is shipped by sea, and 32% of the world fleet controlled by EU companies. With these figures in mind and the actions performed by the European Commission to better engage with maritime stakeholders and modernize the maritime framework in Europe, competitiveness on ports has greatly increased [EUC18]. In addition, the Port Services Regulation has been adopted to set clear and specific rules on transparency of public funding and access to port services, as well as the extension of the General Block Exemption Regulation, makes it possible to have greater flexibility on public investments in ports. The impact of this factor can be considered as positive to Cyber-MAR.

- **Investment in innovative solutions:** EU funds are made available for the uptake of innovative solutions both in the cybersecurity and maritime sectors, responding to the challenges of new digitalization era. Regular calls have been targeted by the EU Commission to the maritime and cybersecurity sectors within the Connecting Europe Facility (CEF) or Horizon 2020 Research and Innovation Framework Programme (H2020). In 2017, the Commission allocated 196 million euros to new maritime projects under the CEF program and 214 million euros under the H2020 program [EUC18]. In addition, a total investment of up to 450 million euros have been allocated to the

[1] https://www.un.org/en/observances/anti-corruption-day
[2] https://www.maritime-acn.org/
[3] https://events.safety4sea.com/2019-safety4sea-awards/

digital Single Market strategy including a public-private partnership (PPP) on cybersecurity during 2017 and 20202 [EUC17]. The impact of this factor for the Cyber-MAR solutions can be considered as very positive.

- **Blue economy:** This is a term that emphasizes conservation and sustainable management based on the idea that healthy ocean ecosystems are more productive and fundamental to sustainable, ocean-based economies. The European Commission has undertaken to measure the trends, performance and progress of the Blue Economy, that in its first annual report looks not only at established maritime sectors (e.g., ports, shipbuilding, transport, etc.), but also some innovative emerging sectors [BLU18]. The Green Shipping Guarantee Programme[4] have been created to accelerate the implementation of investment in greener and sustainable technologies by European shipping companies. The proposed funding of the program covers 750 million euros and it is expected to generate investments of 3 billion euros [EUC18]. However, there is currently a poor security situation in the shipping industry, which creates uncertainty and prevents the full potential of the blue economy; responsible fisheries, oil exploitation, sea transport and even tourism [SAF19]. The impact of this factor in Cyber-MAR can be considered as neutral.

- **EU current economic situation:** Although by 2019, the economic forecast report presented by the EU Commission [SEF19] indicated a moderate growth in the EU economy with an average of 1.2% of the GDP growth in the euro area, providing a positive environment for creating new business and launching new projects, the situation has drastically changed due to the coronavirus (COVID-19) pandemic situation, turning into a deep and uneven recession for the global and EU economies with very severe socio-economic consequences [SEF20].

  Projections on the growth of EU economy estimate that the EU economy will be contracted by 7.5% in 2020 and grow by around 6% in 2021. All EU members have been greatly affected by the pandemic and their recovery will depend not only on the evolution of the pandemic in each country, but also on the structure of their economy and the capacity to respond with stabilizing policies [SEF20].

  Unemployment is set to increase in most EU countries, although policy measures should limit the rise. However, projections on the unemployment rate in the EU is estimated to rise from 6.7% (in 2019) to 9% in 2020 before declining to around 8% in 2021 [SEF20].

  In addition, consumer prices are estimated to fall substantially due to the reduction in the demand and the fall in oil prices. Inflation in the EU is projected to reach 0.6% in 2020 and 1.3% in 2021, according to the Harmonised Index of Consumer Prices (HICP[5]).

  Furthermore, the aggregate government deficit in the EU and euro area in general is expected to increase from 0.6% of Gross Domestic Product – GDP[6] (in 2019) to around 8.5% in 2020, before falling back to around 3.5% in 2021.

  Furthermore, ever since the COVID-19 started, cyber incidents have been on the rise. A spike in phishing attacks, spams and ransomware attacks have been observed, as attackers are using COVID-19 as bait to impersonate brands thereby misleading

[4] https://www.eib.org/en/projects/pipelines/all/20150334
[5] https://www.ecb.europa.eu/stats/macroeconomic_and_sectoral/hicp/html/index.en.html
[6] https://www.imf.org/external/datamapper/NGDP_RPCH@WEO/EU/EURO/EUQ

employees and customers [TOP20]. Statistics show impressive data on the consequences of the COVID-19 in the cybersecurity maritime domain (e.g., with a 400% increase in attempted hacks since February 2020 [NAU20]) which have obliged around 70% of organizations to increase cybersecurity spending [SEC20]. As a result, COVID-19 has had a major impact on global shipping, affecting all shipping sectors from passenger ships to container ships and oil tankers [EMS20].

Finally, without an appropriate and timely recovery strategy to the COVID-19 situation, the risk that the crisis could lead to more severe distortions within the Single Market causing economic, financial and social divergences between EU Member States is one of the major threats to be considered and analysed. The pandemic could cause more severe and permanent changes in attitudes towards global value chains and international cooperation, which would weigh on the highly open and interconnected European economy. The pandemic could also leave permanent scars through bankruptcies and long-lasting damage to the labour market [SEF20], making it a very negative situation to lunch and exploit the Cyber-MAR solution in the market.

- **Business opportunities in the cybersecurity and maritime sectors:** The maritime sector offers an opportunity for development and growth in the Mediterranean. The Union for the Mediterranean (UftM[7]) Secretariat is actively working with all its partners across the region to improve maritime-related sectors via concrete projects and initiatives benefiting both shores of the Mediterranean. With funds that reach 520 million euros, the UfM supports projects (e.g., LOGISMED Training Activities[8], Motorway of the Sea[9], and OPTIMED[10]) aiming to reinforcing transport, logistic and trade connections among the ports of the Mediterranean area [UFM20]. These initiatives are considered as a great option for expanding the developed solutions within the Cyber-MAR project. The impact of this factor can be considered as positive for Cyber-MAR.

- **Direct economic incentives to improve cybersecurity in the maritime sector:** According to analysis presented by the European Network and Information Security Agency (ENISA) about the cybersecurity aspects in the maritime sector [ENI11], back in 2011 there were not enough direct economic incentives to implement good cyber security in the maritime sector. Some relevant stakeholders (e.g., cyber insurance companies) were not engaged to stimulate the development of cyber security practices in the maritime sector. The situation was originated due to the lack of good security baselines and insufficient regulatory framework. However according to the ENISA's Port Security report [ENI19], ports are required 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, the procedures to be followed, the measures to be put in place and the actions to be undertaken. In addition, nowadays all EU states members possess a well-defined national cyber security plan with substantial funds to promote and execute cyber security initiatives in all major sectors

[7] https://ufmsecretariat.org/
[8] https://ufmsecretariat.org/project/ufm-labelled-project-logismedta-to-contribute-to-the-creation-of-jobs-in-the-region-2/
[9] https://ufmsecretariat.org/project/motorway-of-the-sea-mos-turkey-italy-tunisia-project/
[10] https://ufmsecretariat.org/project/optimed-implementation-towards-a-new-mediterranean-corridor-from-south-eastern-to-north-western-ports/

of the economy, including the maritime domain. This factor constitutes, therefore, a very positive aspect to be considered by the Cyber-MAR project.

3.3 Social Analysis

Social factors such as consumer habits and attitudes, education and skills of the target population, as well as awareness and interests on the cybersecurity solutions used in the maritime sector play a significant role in how the market would react to the assets developed as part of the Cyber-MAR project. The following aspects are considered as key social factors to be analysed in the project:

- **Cybersecurity & Maritime stakeholder's relationship:** one of the EU Commission strategy to implement in the cybersecurity and maritime sectors is to intensify the dialogue among stakeholders by (i) organizing high-level events (e.g., conferences, workshops, industrial presentations, forums, etc.), (ii) adopting policies and regulations to prioritize activities in the sector; and (iii) develop synergies among stakeholders intensifying cooperation with multidisciplinary expert groups [EUC18].
  In addition, information sharing mechanisms on threats, incidents and good practices among port operators (port authorities, terminal operators etc.) and between port operators and other maritime stakeholders (e.g., shipping companies) 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.
  Several interesting initiatives are currently being implemented and are a viable option for collaborative private-public initiatives of sharing information on threat intelligence at European level. The S-PORT[11], the Malware Information Sharing Platform (MISP[12]), and the Maritime and Port Security Information Sharing & Analysis Organization (MPS-ISAO[13]) are examples of these initiatives aiming to developing collaborative environments for the security management and information sharing of Ports. Cyber-MAR can benefit from these activities by creating synergies with key stakeholders to strengthen relationships with potential customers. The impact of this factor can be considered as positive for the Cyber-MAR project.

- **Awareness on maritime cybersecurity:** A recent research performed by safety4Sea [SAF19], considers that organizations with healthy cybersecurity culture are about 50% less susceptible to be attacked and 60% less likely to make errors in their work. In addition, awareness on the impact of cyber-attacks against IT and OT infrastructures has greatly increased during the last decade, compared to the assessment performed by ENISA in 2011 [ENI11], where awareness regarding cyber security aspects was established as very low and even non-existent. Today (almost 10 years later), most organizations are aware of the threats and challenges posed by cybersecurity attacks and a great number of them are investing money and time in building a healthy cybersecurity culture.
  Taking into account that organization's security is only as strong as its weakest link, and that awareness could be considered as one of the weakest organization's link, a great attention must be considered to strengthen this aspect. Consequently, a variety of

[11] http://s-port.unipi.gr/index.php/
[12] https://www.misp-project.org/
[13] https://mpsisao.org/about/

training courses and methodologies is currently available online to train staff and crew members into improving their knowledge, skills and awareness about cybersecurity issues in the maritime sector. Cyber security technologies have become essential to the operation and management of systems critical to the safety and security of shipping and protection of the marine environment. An effective cybersecurity strategy and a realistic awareness of cybersecurity threats will privilege prepared organizations with new business opportunities to explore [LLO20, LEE17]. The impact of this factor to the Cyber-MAR project can be considered as positive.

- **EU Education and skills:** Education plays a key role in the Europe 2020 strategy [CEP10]. As EU citizens are more skilled to use and operate new technological devices, habits of resource consumption tend to change more frequently than before. This is mostly defined by the generation to which the individual belongs: Generation X (born between 1965 and 1980), viewed as peer-oriented and entrepreneurial in spirit; Generation Y, a.k.a., millennials (born between 1981 and 1996), have led older generations in technology adoption and embracing digital solutions; Generation Z (born between 1997 and 2010), have grown up with technology and social media making them tech-addicted; and the Generation alpha, (born after 2010) considers technology as deeply integrated in their every day's life [INS19].
  In general, one common aspect among all generations is the interest in new technologies. Although most people can manipulate and use current technological devices, few are qualified enough to operate Security Operation Centres (SOCs) and most cybersecurity tools. There is a shortage of highly skilled engineers, scientists and other cybersecurity specialists to support and lead solutions to current and future industrial-related challenges [CSE20]. A recent research on the cybersecurity labor market in the UK found that most firms suffer basic cybersecurity skills shortage [CIS20]. Furthermore, Cybersecurity Ventures predicts that there will be 3.5 million unfilled cybersecurity jobs globally by 2021 [MOR19]. Similarly, a recent study revealed that Europe faces a huge 350,000 cybersecurity skilled workers gap by 2022 [EMP19]. These events reinforce the identified need for training on cybersecurity solutions in the maritime domain, a very positive opportunity to introduce Cyber-MAR solutions and to explore potential business development within the project.

- **EU Consumer habits:** EU citizens are entitled with the right of free movement that allows them to live, travel and work in any of the EU country members without special formalities. This freedom of movement and residence for EU citizens is the cornerstone of Union citizenship, established by the Treaty of Maastricht[14] in 1992. The Schengen Area guarantees free movement to more than 400 million EU citizens, as well as to many legal residents of EU member states [EUC20], which allows them to receive an equal treatment as the one given to EU nationals regarding employment, working conditions, social security conditions, tax advantages, etc., [EUC20a, EUC20b].
  In addition, EU consumers increasingly use mobile for commerce activities (including banking services). Most of their purchase decisions are motivated by friends, family members and influencers. Furthermore, best price and time savings are top motivations for shopping online, being free shipping one of the most popular features that triggers immediate purchase. However, one of the main barriers to online shopping is the lack of trust in security of online payment methods. This open new issues on the online payment industry, which requires to build, introduce and educate EU consumers about online payment solutions [EVA17].

[14] https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_on_european_union_en.pdf

Currently, more than 90% of cyber-attacks use social engineering techniques to trick users into obtaining their confidential and financial data. Phishing and social engineering, unintentional downloads of malware, etc., are some of the most common issues [DNV20]. People's habits on the use of digital technologies are the main focus of cybersecurity threats.

Although lockdown orders will be lifted eventually, there are thousands and millions of customers whose patterns of purchase have changed drastically for a more comfortable way of getting what they need at their doorstep. They are comfortable with the online system not only for their convenience but also for getting into any risk of catching COVID-19. According to a recent survey on social media, young consumers are more motivated than ever to maintain social distancing and shop online while staying at home. This trend is creating ideal market conditions and great motivation for newly entrant digital entrepreneurs [EHT20]. As a result, this trend on using digital commerce post COVID-19 generates a positive environment to introduce the Cyber-MAR solutions into the market.

3.4 Technological Analysis

Due to the rapid technology advancements to which the maritime industry is exposed and the high ICT complexity, ensuring an adequate maritime cybersecurity strategy has become a major challenge. The first EU-report on maritime cybersecurity produced by ENISA [ENI11] positions these domains as a logical and crucial next step in the global protection efforts of ICT infrastructures. The following technological factors are considered to have a major impact on the activities to be performed in the Cyber-MAR project.

- **Making use of digitalization:** The EU Commission has presented a proposal for the establishment of a digital environment for exchange of information. The proposal entitled establishing a European Maritime Single Window environment in 2018 [EMS18] considers that digitalization of transport can have a positive impact on various areas, including transport management, exchange of information and cost efficiency. The main objectives of such proposal are three-fold: (i) normalize reporting procedures, interfaces and data formats; (ii) reduce time and effort in the ship reporting process by providing a single entry point; and (iii) increase efficiency of digital reporting by facilitating data sharing/reuse [EUP18]. In maritime transport, digitalization can have a direct impact on the reporting obligations for ships calling at EU ports, and will facilitate enforcement and monitoring for safety, environmental and security purposes, including cyber-security [EUC18, EUP18].

  As in many other industries, the maritime domain also provides artificial intelligence to the digitalized objects through the use of programmability, storage capacity, sensors, and networking, which allows an increase in the efficiency of ship operations. With the use of Big Data and digital transformation, the fleet controls can be optimized, whereby costs are reduced, and the environmental protection is improved. Traffic control and traffic flows can be optimized by using the ship's operating data, thereby avoiding critical situations and thus reducing the risk of accidents. However, technology and information ethics ask for the gain and loss of personal and informational autonomy and the dependency of the customers on information technology and information companies. The handling with digital applications and technologies does not only require competent users who are familiar with the digital innovations, but also

secure systems that guarantee the protection of the company's internal infrastructure and operating systems from cyberattacks [FRU17]. These are positive aspects to be considered by technology providers within the Cyber-MAR context.

- **Cybersecurity maturity in Europe:** According to the most recent Global Cybersecurity index [GCI18], Europe is assessed to have a high maturity in cybersecurity related aspects (i.e., legal, technical, organizational, capacity building and cooperation). Most countries have cybercrime legislation, National incident response teams (e.g., CERT, CSIRT), and national cybersecurity strategies (NCS). In addition, many European countries use cybersecurity metrics to measure cybersecurity and are highly engaged in cybersecurity awareness campaigns. Europe is the leading region in providing cybersecurity professional training and in public-private partnerships. The United Kingdom, France and Lithuania provide the top three highest scores in all cybersecurity aspects. Other countries e.g., Estonia, Spain and Norway, belong to the top ten countries with the highest cybersecurity index, making Europe, the most mature region all over the world. However, there are EU countries (e.g., Malta, Greece, Romania, and Czech Republic) whose maturity still does not reach high levels of performance, making this a potential barrier for the Cyber-MAR go to market strategy.
  In addition, there exist considerable discrepancies between EU member states in terms of cybersecurity policies, legal frameworks and operational capabilities, creating notable cybersecurity gaps across Europe. Furthermore, although all EU countries have established operational entities (e.g., CERTs), their mission and experience vary greatly from one entity to another. Although some effort is being coordinated, there is no information sharing mechanism that currently allows all EU members to exchange and share appropriate and meaningful information at the right time about the cybersecurity incidents or breaches they are able to detect [BSA15]. The impact of this element can be considered as negative for the Cyber-MAR project.

- **Rapid advances in technology:** the EU is investing in R&D activities in all technological areas (e.g., Automation, Big Data, Artificial intelligence, Simulation and Modelling, Software, Sustainable Maritime Transport, aiming to improving detection and reaction capabilities against major cyber and physical threats affecting the maritime sector [FRU17]. The EU framework is in continuous modernization, considering aspects to improve safety both on-board and onshore, including the adoption of new rules on the design, construction and performance requirements; testing standards for marine equipment; and the implementation of electronic tagging on marine equipment [EUC18].
  One of the major technological factors to be analysed on the maritime domain is the use of Blockchain technology. Although very beneficial to most businesses since it provides fast and safe transactions at low costs, blockchain is one of the major issues concerning the future of shipping [SAF19]. The totally decentralized, open source, peer to peer software and the management of all transactions, along with the lack of regulations on these matters becomes an important issue to be considered in all industrial areas. This situation is expected to cause advancements in the international trade and supply chain management, and thus, new opportunities for the key players working in the global blockchain market. In 2017, the global blockchain in energy

market was valued at around USD 208 million in 2017 and is expected to reach about USD 12 billion by 2024 [ZIO18].

As shipping becomes more technologically connected, the industry is expected to be transformed into a new business model based on more remote controls, autonomy and requirement simplification [SAF19]. The shipping 4.0 [LAM17, KAV20] is expected to bring a great number of benefits to the industry, their customers and the society as a whole. Among these benefits, safety is expected to be increased while operational and construction costs will be reduced. Environmental and social sustainability is expected to improve, which will make the shipping industry more competitive against other transport modes [BJO16]. The risk of piracy will be reduced, and new business opportunities will arise accordingly. Along with the benefits, **modern control systems and autonomous shipping** increases the cybersecurity attack surface, and thus new technological security issues will arise. The major challenge for implementing fully automated systems controlled by remote operators or by algorithms is not to make them work, but to make them sufficiently safe [EUC18].

Maritime surveillance is an interesting technological factor that impact multiple maritime areas e.g., safety and security, law enforcement, defence, border control, environmental protection, fisheries control, trade and economic interests of the EU. Satellite imagery is used to locate and track vessels, monitor ports and detect malicious incidents in the maritime domain [PAR15]. Several initiatives have been developed to provide maritime surveillance services e.g., PERSEUS[15] (Protection of European seas and borders through the intelligent use of surveillance), PROMERC[16] (Protection measures for merchant ships), SafeSeaNet[17] (Maritime data exchange across Europe), THETIS[18] (information system supporting new Port State Control inspection regime), etc.

Overall technological advances are considered as a positive factor for the Cyber-MAR project due to the challenges they pose to protect the maritime domain against cybersecurity issues, which opens new business opportunities to introduce innovative and robust solutions in the area.

- **Convergence of IT and OT:** While Information Technology (IT) is responsible for the systems that collect, transport and process data that provide information to the business, Operational technology (OT) generally comprises the systems that handle the monitoring and automation of ICT (e.g., automation of machines, processes, and system within a plant). Confidentiality is the primary goal and the most important characteristic of the systems that IT is concerned about, whereas availability is the most critical aspect OT is concerned about [LAG18]. In the maritime domain, losing the sensor data acquired by the SCADA system has a low impact in confidentiality as sensors are publicly displayed on board. However, from a safety point of view, it is important that information transmitted by the sensors is trustworthy, which increases the potential value of integrity. Similarly, if the collected information cannot be properly accessed, availability will be highly impacted, as it may cause a serious safety issue [LAG18].

[15] https://cordis.europa.eu/project/id/261748
[16] https://cordis.europa.eu/project/id/607685
[17] http://www.emsa.europa.eu/ssn-main.html
[18] http://www.emsa.europa.eu/psc-main/thetis.html

In addition, IT systems are widely used in marine transportation, both shipboards and in port/cargo terminals. Their functionalities range from monitoring, to access control, radar, communication, and automation. Many ships have become complex computer-controlled platforms, where the operators have limited physical control over critical systems. The use of digital communications to link seaborne systems to shore-based applications means that the vessels are also part of a hyper-connected world which is dominated by the Internet [BOY13].

To reduce the potential risk to which an industrial system is exposed, it is imperative to converge IT and OT. This sort of approach requires employees from IT and OT to be cross-trained [LAG18]. Consequently, this situation will require solutions as those being developed in Cyber-MAR, which constitutes a very positive aspect to be considered in the project.

- **Vulnerabilities in industrial systems:** Industrial Control Systems (ICS) use completely different protocols compared to the ones used in traditional IT systems (i.e., TCP/IP). ICS protocols are varied and have been developed to communicate over serial media (RS-485[19]) [HAC18]. As a result, conventional security of IT systems is not enough to protect against proliferating cyber threats against OT systems. OT networks have different operational requirements that impact the ability to adapt and respond to new cybersecurity threats which eventually, reveals new vulnerabilities. In general, OT systems lack secure development, they provide low level access protection, they have no procedures or trained staff to check for abnormal activity on their systems, and their communication protocols lack of encryption mechanisms [LAG18]. These vulnerabilities give raise to a variety of malicious incidents such as illegitimate connections to servers; password attacks; malware use to obtain sensitive information about cargo, vessels and their destinations; unauthorized access to information systems which enable smuggling and fraud activities; and the disable or damage of critical ship systems (e.g., navigation, propulsion, emergency communications, life support, etc.) [BOY13]. To properly protect the maritime sector against these malicious events, solutions like those being developed in Cyber-MAR will be highly demanded by key stakeholders, which constitutes a positive factor to be considered in the project.

- **Cyber incident handling process in the maritime domain:** The protection of the maritime sector against cyber and physical threats requires mechanisms and procedures to prevent, detect, respond, mitigate and recover from attacks affecting the confidentiality, integrity and availability of information. Having an established and rehearsed plan of action which a maritime organization executes after identifying a cybersecurity attack is crucial to limiting the damages. An effective plan should cover (i) a preparation phase that considers resilience and security control measures; (ii) a detection & analysis phase that considers abnormal detection that could lead to an early indication of an event before it happens; (iii) a mitigation & recovery phase that considers the elimination of the detected incident and the system being restored to its normal operations; and (iv) a post incident phase, containing reflections and lessons learnt about the incidents, as well as strategies for improvement. A concrete strategy to handle cyber incidents with specific roles and responsibilities for the users, secure procedures, and specific contingency and recovery plans is one of the main challenges

[19] https://www.lammertbies.nl/comm/info/rs-485

the maritime industry is currently facing [OIK19]. Cyber-MAR can take advantage of this fact to introduce its assets and main solutions to potential customers. The impact of this factor in the Cyber-MAR project can be considered as neutral.

3.5 Environmental Analysis

Every action taken to introduce a new solution to the market will have affect (positively or negatively) the environment and thus the market as a whole. Cyber-MAR must consider the following environmental factors before starting new businesses in the maritime cybersecurity market.

- **Vessels for the Future (VftF):** aiming to reducing CO_2 emissions by 80% and SOx and NOx by 100%, as well as reducing risks by a factor of 10, VftF grouped enterprises, research institutions, academic organizations and associations interested in stimulating integration among shipbuilders, suppliers, research centres and classification associations. With a cutting-edge technology, the initiative focuses on improving the safety and efficiency of waterborne transport, and developing a competitive maritime sector in Europe, which will deliver by 2050 a safer and cleaner vision of the European maritime sector [GOV18]. The VftF project brings together Europe's maritime industry in a public private partnership (PPP) and the European Research Association, which is considered as a very positive factor for the Cyber-MAR project.

- **Environmental challenges and issues:** Europe is one of the leading maritime centres on earth with more than 400 million passengers using its ports and services. Besides the uncounted benefits that this sector provides to the national and international economies, there are currently many challenges to which the maritime industry is confronted to, including a real need to limit ship-source pollution, notably greenhouse gas emissions, air pollution or waste from ships. The EU has put in place one of the most extensive and successful legislative framework for safety, environmental protection and quality shipping, which covers the entire chain. The European Maritime Safety Agency provides technical, operational and scientific assistance, and a network of antipollution vessels. In addition, the Agency cooperates directly with national coast guard organizations and other EU agencies such as Frontex[20] and the European Fisheries Control Agency (EFCA[21]) [EMT20]. However, as most of these challenges remain open issues, this situation could impose restrictions and limitations to the appropriate development of the Cyber-MAR solutions, and thus it is considered as a potential negative factor for the project.

- **Environmental protection initiatives:** A great number of initiatives are currently in place to protect the environment from the consequences of the activities performed in the maritime industry. Among these initiatives, decarbonization is one of the priorities. The International Maritime Organization (IMO) is implementing a strategy to reduce shipping emissions of greenhouse gases by 50% by 2050 compared to 2008 while already many organizations are revealing their ambitious plans towards full decarbonization. Similarly, the IMO is highly concerned on preventing the impact of invasive marine species and noise reduction from marine traffic, towards clean seas in Europe. In addition, a safety culture and safety climate are major priorities in shipping

[20] https://frontex.europa.eu/
[21] https://www.efca.europa.eu/en

companies with a focus on training programs, maintenance and risk assessments [SAF19, SMC19]. The UK is actively driving the transition to zero emission shipping in its water, moving faster than competitors and international standards [MAR50]. Cyber-MAR should consider all these initiatives as a positive factor towards the development of its solutions.

- **Climate change:** The maritime sector needs to ensure its performance is sustained and even improved to tackle effectively climate change, air or water pollution. Climate change is an issue that requires a global solution, and the EU is actively engaging within the IMO to prepare strategies to reduce GHG emissions [EMT20]. The Paris agreement is the first-ever universal, legally binding global climate change agreement adopted by the EU member states in 2015. The agreement sets out global framework to avoid dangerous climate change by limiting global warming to well below 2ºC and pursuing efforts to limit it to 1.5ºC [PAA16]. In addition, it helps countries to deal with the impact of climate change and support them in their efforts. The EU Commission also continues to promote high levels of environmental protection in EU waters, coastlines and ports, through the necessary standards, and in supporting the sector to effectively comply with legislation [EMT20]. Organizations are therefore engaged to respect and follow the agreed actions which may impose new restrictions and limitations to the maritime sector. The impact of this factor can be considered as negative for the Cyber-MAR project.

3.6 Legal Analysis

This section considers the different laws and regulations that affect directly and/or indirectly businesses and operations within the cybersecurity and maritime industries, including international and local regulations within the EU state members about data protection, privacy, intellectual property rights, as well as national strategies that regulate the cybersecurity and maritime operations. Cyber-MAR must consider the following legal factors before starting new businesses in the maritime cybersecurity market.

International Context [ENI19]: Several policies and regulations have been designed by international organizations in the context of the maritime cybersecurity sector. The International Maritime Organization (IMO) is responsible for legislation adoptions on maritime safety, environmental pollution prevention, and areas relating to the operation and facilitation of maritime traffic on a worldwide basis. The International Labour Organization (ILO[22]) promotes standards of working and living conditions on board ships, and the United Nations Conference on Trade and Development (UNCTAD[23]) produces international conventions of commercial nature.

The International Ships and Port Facilities Security Code (ISPS[24]) was added to the Safety of Life at Sea (SOLAS)[25] Convention in 2002 to define mandatory requirements and recommendations for ships and port facilities. SOLAS and the Facilitation of

[22] https://www.ilo.org/global/lang--en/index.htm
[23] https://unctad.org/en/Pages/Home.aspx
[24] http://www.imo.org/en/about/conventions/listofconventions/pages/default.aspx
[25] http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

International Maritime Traffic (FAL[26]) conventions defined nine standardized forms for the exchange of information within the maritime ecosystem, considering as mandatory the electronic exchange of required information. This has a strong impact on port IT ecosystems and poses new IT security challenges.

Cybersecurity for the maritime industry has been addressed at International level since 2017 through guidelines and recommendations to the global maritime ecosystem. FAL and the Maritime Security Committee (MSC) defined Guidelines on maritime cyber risk management in MSC-FAL.1/Circ.3.[27] These guidelines make the distinction between IT and OT systems, and recognize that the shipping industry must address relevant security measures by referring to Member Governments' and Flag Administrations' requirements and relevant international or industry standards and best practices (e.g. NIST Framework[28], ISO/IEC 27001[29]).

The international legal framework in the maritime cybersecurity sector is varied but very recent. Laws and regulations have been approved, but their understanding for appropriate implementation is still in its infancy. This factor is therefore considered as neutral for the Cyber-MAR project.

- **EU Regulations** [ENI19]: besides laws and regulations that apply to the international context, several legal frameworks have been defined within the EU. Regulation (EC) 725/2004[30], for instance, 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[31] focuses on enhancing port security. Regulation (EC) 336/2006[32] focuses on the implementation of the International Safety Management Code (ISM[33]) within maritime sector in the EU, and the Directive 2010/65/EU[34] requires that ports of the Member States accept standardized FAL forms to ease traffic. This directive also introduces SafeSeaNet systems[35] established at national and EU level to facilitate secure data exchange between Member States' maritime authorities and other authorities' systems.

  The European Maritime Security Strategy (EUMSS)[36] was defined in 2014 and revised in 2018[37] to be adopted by the General Affairs Council with the objective of identifying, preventing and responding to challenges affecting the security and safety of European citizens, activities and assets in the maritime ecosystem, and thus enhancing awareness among EU member states.

  The Regulation (EU) 2016/679, about the General Data Protection Regulation (GDPR) [GDP16], on the protection requirements of the personal data processing and on the free movement of such data, applied for all sectors, including the maritime sector.

[26] http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/Convention-on-Facilitation-of-International-Maritime-Traffic-(FAL).aspx
[27] http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf
[28] https://www.nist.gov/cyberframework
[29] https://www.iso.org/isoiec-27001-information-security.html
[30] https://eur-lex.europa.eu/homepage.html
[31] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:310:0028:0039:EN:PDF
[32] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1568879842121&uri=CELEX:32006R0336
[33] http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx
[34] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1568879869082&uri=CELEX:32010L0065
[35] http://www.emsa.europa.eu/ssn-main.html
[36] https://ec.europa.eu/maritimeaffairs/policy/maritime-security_en
[37] https://www.consilium.europa.eu/en/press/press-releases/2018/06/26/maritime-security-eu-revises-its-action-plan/

In terms of cybersecurity legislations, the Directive 2016/1148 (NIS Directive)[31] aims to harmonizing national cybersecurity capabilities, cross-border collaboration and the supervision of critical sectors across the EU, and the EU Cybersecurity Act[36] strengthens the position of ENISA on cybersecurity related aspects within the EU and defines an EU-wide cybersecurity certification framework for ICT products, services and processes.

Regarding environmental regulations in the EU, although they have a direct impact on the maritime industry, some areas are still poorly regulated at the local level. Ocean freight, for instance, is the least regulated area among all logistic modes. In some cases, such local level regulations are influenced by political considerations [MAI20].

In general, EU regulations are mature and cover most aspects related to the cybersecurity maritime domain. Policy makers are well defined, and initiatives are in place. There is still a long way to follow, but the EU is advancing positively in this matter. This factor can be, therefore considered as positive for the Cyber-MAR project.

- **EU National Strategies:** 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 [ENI19]. Although not all EU member states have the same level of maturity in their strategies, all of them have defined their own National Cybersecurity Strategy (NCSS) as a key policy feature, aiming to improving the security and resilience of national infrastructures and services. ENISA is actively involved in supporting these strategies by providing guidance and practical tools to the member states to evaluate their strategies [ENI20]. This factor is considered as a very positive aspect for the Cyber-MAR project.

- **General Data Protection Regulation (GDPR):** The GDPR [GDP16] was adopted in May 2016 and, has been applied since May 2018, involving all EU member states into a common framework on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The GDPR defines personal identifiable information as any information relating to an identified or identifiable natural person (e.g., name, ID number, location data, or specific factors related to the physical, mental, economic, or social identity of that person, among others). This implies that metadata related to an individual, e.g., MAC address can be considered PII, which adds a challenge to current businesses.

  In addition, the GDPR states that all system should be created using Privacy-by-Design as default. This implies that data protection should be a major concern in all organizations that process personal data (e.g., storage, usage, exchange*)*. As a result, all digital systems working with personal identifiable data must comply with GDPR by protecting these data and considering security pivotal for their systems.

  Furthermore, the EU Commission has proposed a Regulation on Privacy and Electronic communication, aiming to reinforcing trust and security in Digital Single Market by updating the legal framework on ePrivacy [EPR17]. This latter comes in hand with the GDPR and affects a broader set of players, by applying stronger rules, and having more effective enforcement.

  Even though the GDPR is a relatively new regulation that might create uncertainty regarding compliance and the legal implications in case of alignment failures, this factor can be considered positive for the Cyber-MAR project since as privacy legislation

becomes stronger, the necessity of privacy-preserving tools for data exchange and management will increase accordingly.

- **Brexit and the maritime industry:** Even though there will be an impact on the UK and its relationship with the EU, Brexit will not impede the right of British shipping companies to carry goods to or from EU ports. Considering the UK Government's stated policy on the single market and the customs union, British shipping companies would continue to trade within the EU, but some aspects of this trade might not be as straightforward as they used to be before Brexit. For instance, taxes and duties are very likely to be imposed on goods moving between the EU and the UK, which may affect trade. It also seems highly unlikely that any form of maritime cabotage rights within the EU would be available to UK companies, which could have an impact on shipping companies that operate in these areas. UK shipping companies using EU ports are very likely to be subject to environmental measures whether such measures are adopted or not by the IMO. With the Brexit in place, the UK becomes a third country to the EU, and this will directly affect all the use cases, from data processing, exchange, storage, usage and others [NOR18]. Since there is still great uncertainty over the specificities of Brexit, the impact of this factor can be considered as negative for the Cyber-MAR project.

3.7 PESTEL Mapping and main findings

Figure 2 displays a graphical representation of the PESTEL analysis for the Cyber-MAR project. Each individual factor has been assessed as very positive (+P), positive (P), neutral (X), negative (N), and very negative (+N).

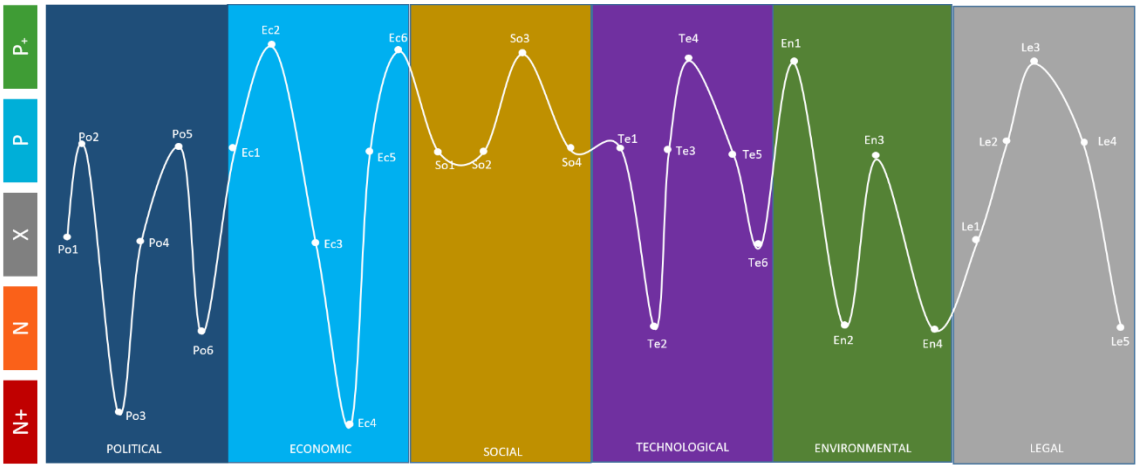


Figure 2. PESTEL Analysis

As can be seen from the previous diagram, most of the PESTEL factors fall into the Positive (P) or Very Positive (+P) categories, which in turn reflects an optimal environment for the Cyber-MAR solutions that can be beneficial for the appropriate introduction of the developed assets into the EU market. However, the following factors may negatively affect the appropriate

development of the Cyber-MAR platform, and should be carefully considered in the exploitation and go to market strategies:

- Current political conflicts between the USA, China, and Russia (among other countries), may affect negatively the trade deals with partners around the world and, ultimately, obstruct shipping by disrupting the value chain and forcing diversion of goods to be processed at the source or in a closer location.
- The current pandemic situation has turned the EU economy into a deep and unforeseen recession with severe socio-economic consequences that would affect negatively the development and evolution of the Cyber-MAR project and solutions. An appropriate and timely strategy to the COVID-19 situation in the EU region is needed to avoid a more severe impact by supporting international cooperation towards a highly open and interconnected EU economy.
- The different levels of cybersecurity maturity in Europe, in terms of policies, legal frameworks, operational capabilities, and technological aspects, creates a potential barrier for the Cyber-MAR go to market strategy. Strategies to reduce these discrepancies among EU member States by establishing common policies and adopting common standards are highly required.
- By observing the rapid cybersecurity technology adoption in the maritime sector, the exploitation team will request more details about the value proposition related with Cyber Ranges and will research in detail the market sector dedicated to training in this area, to improve positioning of our developed solutions.
- Although environmental protection and quality of shipping have been reinforced, climate change and current environment challenges (e.g., limit ship-source pollution, greenhouse gas emissions, air pollution or waste from ships) are open issues that remain unaddressed in the EU and that could negatively affect the appropriate go to market strategy developed for Cyber-MAR. It is therefore important to consider these aspects all over the development of the maritime cybersecurity solutions.
- Taking into account the legal and regulatory evolution, both in the international and EU contexts, where several policies and regulations have been designed by international organizations in the maritime cybersecurity sector, specific exploitation strategies should be defined per sector (e.g., shipping, ports, cybersecurity), considering the different groups and subgroups of Cyber-MAR stakeholders.

4. Stakeholder Analysis

The Stakeholder analysis is a three-fold process that covers the stakeholder identification, understanding and mapping. The analysis initiates by identifying general stakeholders relevant to the Cyber-MAR project. The next step looks to go deeper into understanding these stakeholders. This process considers the Mendelow Matrix, also known as Power/Interest Matrix [ERI18, SLA14]. It assists in grouping the stakeholders in order to identify how to efficiently deal with the relevant project stakeholders to maximize the project's success on the market. The final step of the analysis process maps and prioritize the stakeholders in a power and interest matrix that is further used to build a detailed communication and exploitation plan.

4.1 Stakeholder Identification

This section encompasses the identification of the main stakeholders that are directly or indirectly affected by the Cyber-MAR project. They are grouped as internal stakeholders, including consortium partners (i.e., technology providers, research and academia, and end-users); and external stakeholders, including cybersecurity, shipping and port organizations, (e.g., clients, providers, competitors, etc.) in the cybersecurity and maritime domain. Figure 3 depicts this classification.

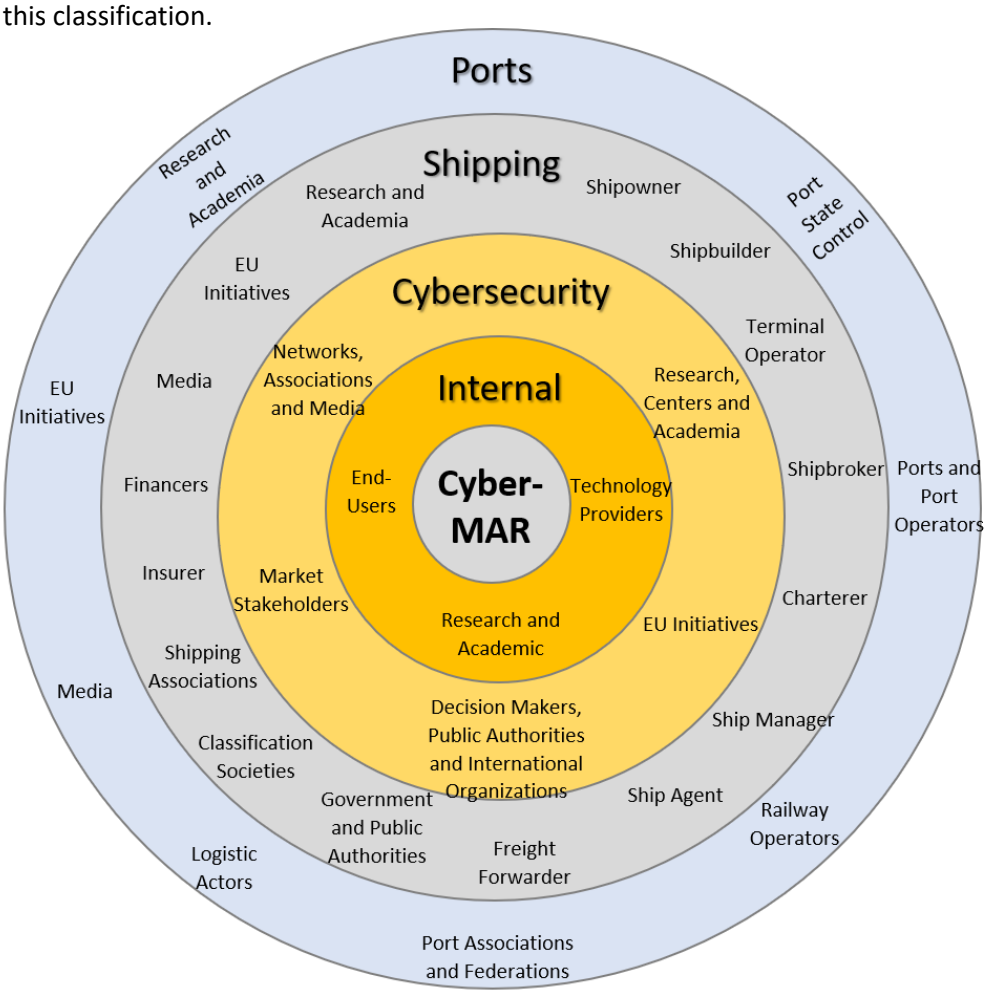


Figure 3. Cyber-MAR Stakeholders Map

The stakeholder identification will be complemented by the identification of the main markets to commercialize the Cyber-MAR solutions. As such, this section provides the initial steps to define the solution and identify exploitation and commercialization routes by means of the identification of potential markets and stakeholders. The remainder of this section details the identified Cyber-MAR stakeholders.

4.1.1 Internal Stakeholders

This category corresponds to internal organizations and key stakeholders directly related to the Cyber-MAR project. It includes organizations directly affected by the developments of assets and services within the project. In this group we can distinguish three main group of stakeholders: (i) project technology providers, (ii) research and academic partners, and (iii) project end-users. Table 2 details each type of internal Cyber-MAR stakeholders.

Table 2. Cyber-MAR Internal Stakeholders

N	Stakeholders	Description
1	**Project Technology Providers**	***DIATEAM, ATOS, AIR, NG*** will contribute to the Cyber-MAR project with software and hardware technology and components to cyber-range platforms to be used for training people, testing new technologies, and measuring procedures to be followed after the detection of a cyber-attack. The technologies of these organizations are the core of the Cyber-MAR architecture
2	**Research and Academic Partners**	***ICCS, VTT, FAIMM, UoP, WMU, SEABILITY*** will contribute with their knowledge, experience and cyber-range tools to improve situational awareness and perform cybersecurity analysis in the maritime domain.
3	**Project End-Users**	**PCT, VPF, PEARL** will provide maritime infrastructures to test and validate the Cyber-MAR solution as well as to improve training activities to ports and shipping stakeholders about the tools and procedures developed in the project

4.1.2 External Stakeholders

This category corresponds to organizations, other than those integrating the project's consortium that affect directly and/or indirectly the activities performed in the Cyber-MAR project. They are categorized in three main groups: cybersecurity, shipping and ports.

- **Cybersecurity Stakeholders:** This category includes international organizations, market companies, international initiatives, public authorities, as well as policy and decision makers affecting the activities performed in the Cyber-MAR project. Tables 3 to 7 detail each type of cybersecurity external stakeholders.

Table 3. Decision Makers, Public authorities and International Organizations

N	Stakeholders	Description
1	**European Commission**	It is the Executive government of the European Union, responsible for proposing legislation, implementing decisions, upholding the EU

	(EC[38])	treaties and managing the day-to-day business of the EU.
2	**European Union Agency for Cybersecurity (ENISA[39])**	It is an organization actively contributing to European cybersecurity policy, supporting Member States and European Union stakeholders to support a response to large-scale cyber incidents that take place across borders in cases where two or more EU Member States have been affected.
3	**European Cyber Security Organisation (ECSO[40])**	is the private counterpart to the European Commission in implementing the contractual Public-Private Partnership (cPPP) on cybersecurity. ECSO's main goal is to develop a competitive European cybersecurity ecosystem, to support the protection of the European Digital Single Market with trusted cybersecurity solutions, and to contribute to the advancement of the European digital autonomy.
4	**International Standardization Bodies**	The Cyber-MAR consortium will be in direct contact with standardization entities and the produced deliverables will be compatible with latest standard activities of the European Telecommunications Standards Institute (ETSI[41]) and the International Organization for Standardisation (ISO[42]).
5	**Cybersecurity national officers and agencies**	EU member states have a national cybersecurity agency aiming to developing cybersecurity and digital trust in citizens, academic and research networks, professionals, enterprises, and strategic sectors to the national and international levels. Examples of these stakeholders are: INCIBE[43] (Spain), ANSSI[44] (France), BSI[45] (Germany), NCSA-FI[46] (Finland), MSB[47] (Sweden), etc.

Table 4. Market Stakeholders

N	Stakeholders	Description
1	**Regulatory Organizations**	This category includes organizations focused on cybersecurity regulation, consumer protection, market regulations, consumer management, service quality controls, compliance, etc. Four major regulations within the EU include the ENISA, the Directive on Security of Network and Information Systems (NIS Directive[48]), the EU Cybersecurity Act[49], and the EU General Data Protection Regulation (GDPR[50]).
2	**Engineering/ consultancy**	Being part of advanced analytical services on the network performance and risk monitoring and control, these stakeholders are key partners on matters of information selection and visualization due to their needs to interpret and link the information to configure and secure IT and OT infrastructure assets.
3	**ICT companies**	Large ICT companies often provide their own cyber ranges, Security Operations Centre (SOCs) and security management tools (e.g., SIEMs).

[38] https://ec.europa.eu/info/index_en
[39] https://www.enisa.europa.eu/
[40] https://ecs-org.eu/about
[41] http://www.etsi.org/
[42] https://www.iso.org/
[43] https://www.incibe.es/en/what-is-incibe
[44] https://www.ssi.gouv.fr/en/
[45] https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html
[46] https://www.kyberturvallisuuskeskus.fi/en/our-activities/ncsa
[47] https://www.msb.se/en/
[48] https://www.enisa.europa.eu/topics/nis-directive
[49] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
[50] https://gdpr-info.eu/

		Cyber-MAR could offer these companies the possibility of making interoperable and holistic the risk management process. Examples of these companies are Microsoft Cyber Defense Operations Center (CDOC[51]), Accenture[52], Paloalto[53], IBM[54], etc.
4	**Cybersecurity SMEs**	SME companies focused on developing cybersecurity tools could be a potential customer/partner of the Cyber-MAR platform. Examples of these companies are AT&T Cybersecurity[55], LogPoint[56], OPAQ[57], Panorys[58], Microsystems[59], etc.
5	**Cyber Insurance Organizations**	Cyber Insurers play a key role in increasing cyber resilience, not only in providing insurance, but also in helping their clients prevent cyber risks and mitigate their impact when they materialise [INS17, ENI12]. Examples of these stakeholders are Allianz Group[60], Zurich Insurance Group[61], AXA XL SA[62], Lloyd's of London Group[63], etc.

Table 5. EU Initiatives

N	Stakeholders	Description
1	**Contractual public-private partnerships (cPPPs[64])**	It is an initiative that helps to tackle societal challenges, including climate change, and to support energy and resource efficiency, and to boost digital innovation and security. There are ten cPPPs between the EU and business representatives which have strategic importance for European industry. Cybersecurity is one of the ten cPPPs.
2	**Cybersecurity and Maritime EU Projects**	With funds allocated from the European Commission in H2020 and Horizon Europe calls, these projects focus on the research and development of cybersecurity solutions to improve the critical infrastructure domains, including the maritime area. Examples of these initiatives are[65]: CYBERWISER, THREAT-ARREST, FORESIGHT, PALAEMON, HiSEA, HOLISHIP, SAURON (more details of each project can be found in Annex 1.

Table 6. Research Centres and Academia

N	Stakeholders	Description
1	**Universities**	This category involves universities (not belonging to the Cyber-MAR consortium but in direct contact with the consortium partners) specialized in the cybersecurity domain. These stakeholders can work in collaboration with the Cyber-MAR consortium in that the research and development of cybersecurity solutions applied to critical

[51] https://www.microsoft.com/en-us/msrc/cdoc
[52] https://www.accenture.com/us-en
[53] https://www.paloaltonetworks.com/solutions/initiatives/cyberrange-overview
[54] https://www.ibm.com/us-en/marketplace/ibm-qradar-siem
[55] https://cybersecurity.att.com/
[56] https://www.logpoint.com/en/
[57] https://opaq.com/
[58] https://www.panorays.com/
[59] http://www.micro-systems.org/services/security/
[60] https://www.allianzgloballife.com/en_IS/allianz-group.html
[61] https://www.zurich.com/
[62] https://axaxl.com/
[63] https://www.lloyds.com/
[64] https://ec.europa.eu/programmes/horizon2020/en/contractual-public-private-partnerships
[65] https://ec.europa.eu/easme/en/european-maritime-and-fisheries-fund-0

		infrastructures including the maritime sector. Examples of these stakeholders are: University of Genoa (UNIGE[66]), University of Rijeka (UNIRI[67]), Universidad Politécnica de Madrid (UPM[68]), University of Sheffield[69], etc.
2	**Research centres and institutes**	This involves institutions and research centres specialized in the field of cybersecurity, aiming to strengthening collaborations in the project's tasks and activities, especially in cybersecurity simulations and defence mechanisms. Examples of these stakeholders are: The Competence Center for IT Security (KIS[70]) & Cybersecurity Competence Center (C3[71]), Center for Applied Security Technology (CAST[72]), etc.
3	**Laboratories**	This category includes research laboratories working in the field of applied cybersecurity, where new applications are developed, tested and made ready for the market. Examples of these labs are the FZI Living Lab SmartSecurity[73], SAMOVAR[74], ZTE Cybersecurity Lab[75], etc.
4	**Student communities**	It covers all associations and communities integrated by students of careers related to information security, cybersecurity, and innovation technologies. These stakeholders can be beneficial to the project by integrating main results and findings into their teaching or training activities (e.g. as part of their Master and Ph.D. theses).

Table 7. Networks, Associations and Media

N	Stakeholders	Description
1	**Networks and Associations**	This category comprises associations of people with mutual interests of the cybersecurity industry aiming to promoting activities to improve cybersecurity awareness in critical infrastructures, with a special focus on the shipping and ports stakeholder community. Examples of these stakeholders are: Forum of Incident Response and Security Teams (FIRST[76]), The SANS Institute[77], Information System Security Association (ISSA[78]), Center for Internet Security (CIS[79]), SEA Europe[80], etc.
2	**CERT/CSIRT Networks**	This category involves both Computer Emergency Response Teams and Computer Security Incident Response Teams in Europe and its member states that can collaborate in activities related to the Cyber-MAR project. Examples of these stakeholders are CERT-EU[81], CERT-France[82] CERT-Austria[83], CERT Belgium[84], CSIRT Italy[85], CERT Sweden[86], etc.

[66] https://unige.it/en/
[67] https://uniri.hr/en/home/
[68] http://www.upm.es/internacional
[69] https://www.sheffield.ac.uk/
[70] https://www.fzi.de/en/research/competence-center-for-it-security/
[71] https://www.cybersecurityintelligence.com/cybersecurity-competence-center-c3-4810.html
[72] https://www.cybersecurityintelligence.com/competence-center-for-applied-security-technology-cast-2811.html
[73] https://www.fzi.de/en/research/fzi-house-of-living-labs/fzi-living-lab-smartsecurity/
[74] https://www.telecom-sudparis.eu/en/research/laboratories/
[75] https://www.zte.com.cn/global/about/news/20190710e1
[76] https://www.first.org/
[77] https://www.sans.org/
[78] https://www.issa.org/
[79] https://www.cisecurity.org/
[80] http://www.seaeurope.eu/
[81] https://cert.europa.eu/
[82] https://www.cert.ssi.gouv.fr/
[83] https://cert.at/en/home/
[84] https://cert.be/en
[85] https://www.csirt-ita.it/
[86] https://www.cert.se/om-cert-se

3	**IoT/Big Data Associations**	The Cyber-MAR project could be positioned as a technology development to integrate cybersecurity, maritime, and risk management to improve the protection of shipping and port resources involving IoT devices and Big Data. In Europe, the Alliance for Internet of Things Innovation (AIOTI[87]) or the Big Data Value Association (BDVA[88]) are interested in expanding the adoption of IoT technology as well as creating alliance between several domains to develop and use common architectures.
4	**Local and European media**	This category involves all kind of regional and European media discussing on aspects related to cybersecurity. This includes, electronic & print news, local press agencies, EC magazines (electronic & print), Journalists & bloggers, among others. Examples of these stakeholders are: IT Security Guru[89], The hacker News[90], Infosecurity Magazine[91], etc.

- **Shipping Stakeholders:** This category includes stakeholders in the shipping process (e.g., shipowner, ship agent, freight and forwarder, classification societies, etc., that are directly and/or indirectly affected by the activities performed in the Cyber-MAR project. Table 8 details this type of stakeholders.

Table 8. Shipping Stakeholders

N	Stakeholders	Description
1	**Shipowner**	Individual or company who, equips and exploits a ship, to transport passengers or to deliver cargo at a certain freight rate. Examples of this type of stakeholders are Mediterranean Shipping Company (MSC[92]), Global Container Shipping Company (MSC Spain[93]), Grandi Mavi Veloci (GNV[94]), Costa[95], Tallink[96], Viking Line[97], Finnlines[98], Eckero Line[99], etc.
2	**Shipbuilder**	It receives orders from shipowners to construct ships based on ships' specifications. It includes ship technicians e.g., ship repair, ship maintenance.
3	**Terminal Operator**	Companies that move cargo through a port at contracted minimum level of productivity
4	**Shipbroker**	Specialists intermediaries/negotiators between shipowners and charterers (including sale and purchase, demolition, liner chartering, tramp chartering).
5	**Charterer**	Companies that either own a cargo and employ a shipbroker to find a ship for the cargo delivery, or a party without a cargo that hires a vessel or charter for a specific period to carry cargoes at a profit above the hire rate. Examples of charters: bare Boat Charter, Time Charter, Single Voyage/Spot Charter.

[87] https://aioti.eu/
[88] http://www.bdva.eu/
[89] https://www.itsecurityguru.org/
[90] https://thehackernews.com/
[91] https://www.infosecurity-magazine.com/
[92] https://www.msc.com/?lang=en-gb&local=false
[93] https://www.msc.com/esp
[94] https://www.gnv.it/en
[95] https://www.costacruises.com/
[96] https://www.tallink.com/
[97] https://www.vikingline.com/
[98] https://www.finnlines.com/
[99] https://www.eckeroline.com/

6	**Ship Manager**	In charge of the duties a shipping company must perform for the technical or commercial operation of a vessel, such as: crew management, logistics, vessel chartering
7	**Ship Agent**	A person who deals with the transactions of a ship in every port that the ship visits or docks and takes care of every need and requirement of the crew like getting local currency, getting the mail, any repairmen in case the ship requires major repairing, refilling the food and water containers and many other such duties.
8	**Freight Forwarder**	A person or company that organizes shipments for individuals or corporations to get goods from the manufacturer or producer to a market, customer or final point of distribution.
9	**Government and Public Authorities**	Maritime administrations or flag state administrations responsible for carrying out the shipping responsibilities of the state and are tasked to administer national shipping and boating issues and laws within their territorial waters and for vessels flagged in that country, or that fall under their jurisdiction. Examples of stakeholders in this category are: The European Maritime Safety Agency (EMSA[100]), the International Maritime Organization (IMO[101]), etc.
10	**Classification Societies**	Non-governmental organizations that establishes and maintains technical standards for the construction and operation of ships and offshore structures. They classify and certify marine vessels and structures based on their structure, design and safety standards. Examples of these societies in Europe are Lloyd's Register[102] (UK), Bureau Veritas[103] (France), Registro Italiano Naval[104] (Italy), DNV GL[105] (Norway), Hellenic Register of Shipping[106] (Greece), etc.
11	**Shipping Associations[107]**	National and international associations created to promote shipping in a wider scale. Examples of these associations are: The International Chamber of Shipping (ICS[108]), The European Community Shipowners' Association (ECSA[109]), The international Tanker Owners Association (Intertanko[110]), The International Parcel Tankers Associations (IPTA[111]), The World Shipping Counsil (WSC[112]), The International Association of Dry Cargo Shipowners (Intercargo[113]), Confitarma Shipowners' Association[114], Assagenti Association[115], etc.
12	**Insurer**	Marine insurance companies that apply to the ship and its operation, along with the risk associated with the transportation of goods by sea. Examples: Hull and Machinery (H&M) Insurance, Cargo insurance, Protection and Indemnity (P&I) Insurance.
13	**Financers**	Financial organizations dealing with the uncertainty over the repayment of the general loan and payment of interest in full on the

[100] http://www.emsa.europa.eu/
[101] http://www.imo.org/en/pages/default.aspx
[102] https://www.lr.org/en/
[103] https://group.bureauveritas.com/
[104] https://www.rina.org/en
[105] https://www.dnvgl.com/
[106] https://hellenicregister.org/
[107] https://shipinsight.com/articles/main-shipping-organisations
[108] http://www.ics-shipping.org/
[109] https://www.ecsa.eu/
[110] https://www.intertanko.com/
[111] https://www.ipta.org.uk/
[112] http://www.worldshipping.org/
[113] https://www.intercargo.org/
[114] https://www.confitarma.it/confitarma-italian-shipownersassociation/
[115] https://www.assagenti.it/en/

		promised date (credit or default risks). Bank loans are granted by a number of different financial institutions e.g., export-import banks, development banks, banks specializing in shipping, commercial banks, shipyard credit, stock exchanges, etc.
14	**Research and Academia**	This category involves universities, research centres, laboratories and/or student communities, (not belonging to the Cyber-MAR consortium, but in direct contact with the consortium partners) specialized in the maritime and shipping domains. Examples of these stakeholders are: Klaipeda Shipping Research Centre (KSRC[116]) , Maritime University of Szcecin[117], Maritime Institute Willem Barentsz[118], etc.
15	**Media**	This category involves all kind of regional and European media discussing on aspects related to the shipping industry. This includes, electronic & print news, local press agencies, EC magazines (electronic & print), Journalists & bloggers, among others. Examples of these stakeholders are: Assoarmatori Magazine[119], World Maritime News[120], Coast Guard Maritime Commons[121], etc.
16	**EU Initiatives**	This category involves European initiatives that work along with ship owners, ship managers, ship operators, equipment manufacturers, and all maritime and shipping stakeholders. Examples of these stakeholders are: Maritime Projects[122], European Maritime and Fisheries Fund (EMFF[123])

- **Port Stakeholders:** This category includes stakeholders such as port state controls, port operators, railway operators, port associations, logistic actors, etc., that are directly and/or indirectly affected by the activities performed in the Cyber-MAR project. Table 9 details this type of stakeholders.

Table 9. Port Stakeholders

N	Stakeholders	Description
1	**Port State Control and Authorities**	This category involves Port State Controls and Port authorities, aiming to inspecting foreign-registered ships in ports other than those of the flag states and take action against ships that are not in compliance. EU countries signed the Paris Memorandum of Understanding on Port State Control (Paris MoU[124]) to establish port state control. Examples of port authority stakeholders are: PAB (Barcelona[125]), PAV (Valencia[126]), PAL (Livorno[127]), Luka Koper (Koper[128]), SPG (Genoa[129]), etc.

[116] http://www.golng.eu/en/project-partners/klaipeda-shipping-research-centre/
[117] https://www.am.szczecin.pl/en
[118] https://www.nhlstenden.com/miwb
[119] http://www.ship2shore.it/it/tag/Assoarmatori
[120] https://worldmaritimenews.com/
[121] https://mariners.coastguard.blog/
[122] http://maritimeprojects.no/about/
[123] https://ec.europa.eu/fisheries/cfp/emff_en
[124] https://www.parismou.org/
[125] http://www.portdebarcelona.cat/en/web/autoritat-portuaria/organizacion
[126] https://www.valenciaport.com/en/
[127] https://www.portialtotirreno.it/
[128] https://www.luka-kp.si/eng/
[129] http://servizi.porto.genova.it/en/home.aspx

2	**Ports and Port Operators**	This category includes EU ports and port operators considered as potential end-users of the Cyber-MAR solutions. These stakeholders can help the consortium on testing, evaluating and providing user feedback of the developed assets. Examples of these stakeholders are: Port of Helsinki[130], Port of HaminaKotka[131], Port of Rauma[132], Port of Oulu[133], Port of Pori[134], Port of Turku[135], Euroports[136], etc. Please note that Port of Valencia and Port of Piraeus are also part of this category. However, due to their implication in the Cyber-MAR project as end-users, they have been included as internal stakeholders in the cybersecurity category.
3	**Railway Operators**	This category covers port railway operators as potential stakeholders of the Cyber-MAR project based on their transportation services they provide and the connection with ports and shipping stakeholders. Examples of this type of stakeholders are Hamburg Port Railway[137], PortShuttle Rotterdam[138], SIBPort[139], etc.
4	**Port Associations and Federations**	Similar to the cybersecurity and shipping associations, this category involves national and international associations created to represent ports and promote its activities in a wider scale. Examples of these stakeholders are: International Cargo Handling Coordination Association (ICHCA[140]), International Association of Ports and Harbors (IAPH)[141], Assiterminal[142], Federation of European Private Port Companies and Terminals (FEPORT)[143], European Federation of Inland Ports (EFIP[144]), etc.
5	**Logistic Actors**	This category includes stakeholders involved in the port logistic, such as warehousing, national transportation, loading and unloading services, port consignments, etc. These stakeholders provide the link between international transportation and the last-mile supply chain services. Examples of logistic actors are: ALGEPOSA[145], StockCargo Group[146], Euro Logistic[147], Bergé Logistics[148], etc.
6	**Media**	This category involves all kind of regional and European media discussing on aspects related to the port industry. This includes, electronic & print news, local press agencies, EC magazines (electronic & print), Journalists & bloggers, among others. Examples of these stakeholders are: The Port Technology International Journal[149], Port Strategy Magazine[150], Port Economics News[151] etc.

[130] https://www.portofhelsinki.fi/en
[131] https://www.haminakotka.com/
[132] https://www.portofrauma.com/en
[133] https://ouluport.com/en/home/
[134] https://www.portofpori.fi/en
[135] https://www.portofturku.fi/en/
[136] https://www.euroports.com/
[137] https://www.hamburg-port-authority.de/en/port-railway/
[138] https://portshuttle-rotterdam.com/en/
[139] http://sibport.es/en/
[140] https://ichca.com/
[141] http://www.iaphworldports.org/
[142] https://www.assiterminal.it/
[143] https://www.feport.eu/
[144] https://www.inlandports.eu/
[145] http://www.algeposagrupo.com/en/maritime-and-port-logistics
[146] http://stockcargo.eu/
[147] https://www.eurologport.eu/
[148] https://bergelogistics.com/
[149] https://www.porttechnology.org/
[150] https://www.portstrategy.com/
[151] https://www.porteconomics.eu/

7	**EU Initiatives**	This category involves initiatives of the European port sector to improve communications, transportation and all related port services within Europe. Examples of these stakeholders are: EcoPorts[152], European Sea Ports Organization (ESPO[153]), Trans-European Transport Network (TEN-T)[154], etc.
8	**Research and Academia**	This category involves universities, research centres, laboratories and/or student communities, (not belonging to the Cyber-MAR consortium, but in direct contact with the consortium partners) specialized in the maritime and port domains. Examples of these stakeholders are Escola Náutica Infante D. Henrique[155], Nikola Vaptsarov Naval Academy[156], University of Portsmouth[157], Escola Europea – Intermodal Transport[158], etc.

4.2 Stakeholder Understanding

Going deeper in the understanding of the various identified Cyber-MAR stakeholders we continue with a mapping and understanding on their positioning around the project. To strengthen the analysis, a first interaction with some of these stakeholders have been performed by some of the Cyber-MAR partners which helps to revaluate the analysis and has helped to design a mature Stakeholder Model.

Using the Power/Interest Matrix (depicted in Figure 4), we are able to map Cyber-MAR stakeholders according to the two axes “power” and “interest”:

The ***Power-axis*** indicates how much impact the respective stakeholder has over the success or failure of the project. This could be because he/she is a direct project sponsor that could stop the project – probably even due to reasons that do not lie in the topic of the project but are rather formal or bureaucratic.

The ***Interest-axis*** indicates how much a particular stakeholder cares about the outcome of the project. A stakeholder that is very interested in the outcome, as he would like to use the technical solution that is being developed, does not necessarily have power over the success or failure of the project.

[152] https://www.ecoports.com/
[153] https://www.espo.be/
[154] https://ec.europa.eu/transport/themes/infrastructure/ten-t_en
[155] https://www.enautica.pt/en/
[156] http://www.naval-acad.bg/en
[157] https://www.port.ac.uk/research/research-centres-and-groups/centre-for-european-and-international-studies-research
[158] http://www.portdebarcelona.cat/en/web/Comunitat-Portuaria/escola

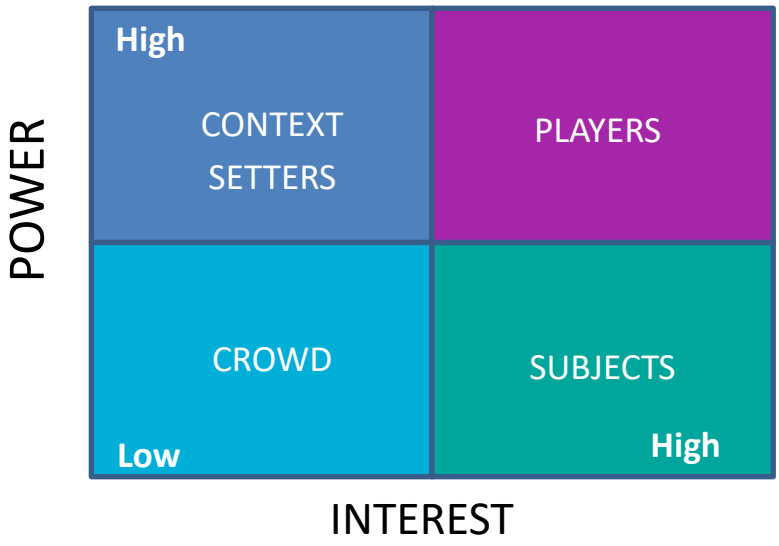


Figure 4. Power-Interest Quadrants

Using the Power/Interest Matrix we classify stakeholders into four dimensions [RED18]:

- **Key Players:** Stakeholders in this category have High Power and High Interest over the Cyber-MAR project. These are your key stakeholders as they have a lot of influence and a strong interest in the outcomes.
- **Context Setters:** Stakeholders in this category are identified as highly influential (high power) but with little interest in the Cyber-MAR project. They may have significant influence over the success of the project but may be difficult to engage with. As such, particular effort may be necessary to engage this group in the activities performed in the project.
- **Subjects:** These stakeholders have high interest and low power over the project. They may be affected but lack of power, and although by definition they are supportive, they are unlikely to be able to play a significant role in implementing the findings of the project. They may however, later become influential by forming alliances with other more influential stakeholders.
- **Crowd:** This category represents those stakeholders with low interest and low power over the project. There is little need to consider them in much detail or to engage with them. However, as the project evolves, their interest or influence may change, therefore it is important to keep an eye on them.

Using a free online tool [MYB20], we have populated the Power/Interest Matrix with the Cyber-MAR stakeholders identified in Sec 4.1., based on their power and interest to the project. For our stakeholder analysis matrix, we have used a scale from 0 (very low interest / power) to 10 (very high interest / power). Table 10 summarizes the assessment used in the matrix.

Table 10. Cyber-MAR Stakeholders Power(P) and Interest (I) Assessment

Cybersecurity	P	I	Shipping	P	I	Ports	P	I
Partner Technology Providers	6	10	Shipowner	4	6	Ports and Port Operators	3	5
Research & Academic Partners	6	9	Shipbuilder	3	8	Port state Control	4	4
Project end-Users	6	8	Terminal Operator	4	7	Railway Operators	3	4
Decision Makers, Public Authorities & International Organizations	8	4	Ship Manager	5	5	Port Associations	2	3
Market Stakeholders	5	6	Ship Agent	5	4	Port Logistic Actors	5	6
EU Initiatives	6	5	Charterer	2	4	Port Research and Academia	3	4
Cybersecurity Research and Academia	4	5	Shipbroker	4	3	Port media	5	5
Networks, Associations and Media	6	4	Freight Forwarder	2	5	Port EU Initiatives	4	5
			Government	10	4			
			Classification Societies	8	3			
			Shipping Associations	3	3			
			Insurer	2	2			
			Financers	7	6			
			Shipping Research and Academia	3	6			
			Shipping media	5	4			
			Shipping EU Initiatives	5	5			

The resulting Power/Interest Matrix is depicted in Figure 5.

Figure 5. Cyber-MAR Power-Interest Matrix

4.3 Stakeholder Management

After generating the power and interest scores and displaying all stakeholders on the matrix, we will be able to identify various strategies to manage and meet their needs. There are different strategies depending on the interest and power levels.

Players: High Power & high Interest => Manage closely

- A full cooperation with these stakeholders is essential in order to get their support all along the project. This group includes not only internal Cyber-MAR partners (i.e., technology providers, academic partners and end-users), but also market stakeholders,

EU initiatives, port logistic actors, port media, and financers, that have been identified as key intermediary to deliver the solutions to end-users.
- Build strong relationships with them and ensure we retain their support.
- Develop partnership strategies to use these stakeholders as Cyber-MAR selling channels.
- Involve them in decisions and engage regularly.

Context Setters: High Power & low Interest => Keep informed

- This group includes shipbuilder, shipowner, terminal operator, freight forwarder, cybersecurity research academia, ports and port operators, port/shipping EU initiatives, shipping research and academia. A recommended strategy is to identify and meet their specific needs to increase their interest towards the project as well as to prevent future conflicts.
- Anticipate their needs and keep these stakeholders informed to ensure their continued support.
- Consult on their area of interest and use their input to improve the project's chances of success.
  Ex: Building a dashboard to keep top management informed about the project's progress / Sharing best practices and lessons learned with the teams.
- Keep these stakeholders informed, but in a very high-level and concise way to avoid them becoming bored/overwhelmed with messages.

Subjects: Low Power & high Interest => Keep satisfied

- This group includes decision makers, public authorities and international organizations, network associations and media, government, classification societies, ship agent, ship manager. Monitoring these stakeholders can bring many benefits in case one of them increases their power level.
- Consider their objectives and keep them satisfied to ensure they remain strong advocates.
- Getting them offside poses a risk. Ex: Sending a monthly newsletter to keep them informed about the progress of the project.
- Adequately inform these people and talk to them to ensure that no major issues arise. People in this category can often be very helpful with the details of the project in a supportive role.

Crowds: Low Power & low Interest => Monitor

- This group includes a variety of maritime transport operators and intermediaries e.g., charterer, shipbroker, shipping associations, insurer, shipping media, port state control, railway operators, port associations, port research and academia that use a limited number of system integrators (generally big companies from the defense sector). An appropriate strategy for Cyber-MAR would be to monitor these stakeholders and consider a business model that includes sells through these integrators.
- Keep an eye on their activity from time to time to stay on top of their involvement. Their relevance may change over time.
- Communicate to keep them informed and encourage their interest, e.g., redoing the stakeholder analysis once in a while to monitor progress with these stakeholders.

5. Cyber-MAR Ecosystem in Europe

This section analyses the current cybersecurity and maritime situation in Europe, focusing on the national strategies and plans developed by several European countries. Taking advantage of the fact that the Cyber-MAR consortium is form of 13 organizations that belong to eight European countries (as seen in Table 11), the ecosystem analysis considered these countries as the main actors to which a questionnaire has been conducted (see Annex 2) in order to identify aspects related to the regulatory framework, initiatives, challenges and existing gaps.

Table 11. Cyber-MAR Ecosystem Participants

LIST OF PARTICIPANTS		
NO.	**COUNTRY**	**RESPONSIBLE PARTNER**
1.	Finland	VTT
2.	France	DIATEAM, Naval Group
3.	Germany	AIR
4.	Greece	ICCS, PCT, Seability, PEARL
5.	Italy	FAIMM
6.	Spain	ATOS, Valencia Port Foundation (VPF)
7.	Sweden	World Maritime University (WMO)
8.	UK	University of Plymouth (UoP)

The remainder of this section separates the cybersecurity the maritime ecosystem analysis in two main blocks for the selected European countries.

5.1 Cybersecurity Ecosystem

5.1.1 Finland

General Information

Finland has a National Cybersecurity Authority, namely NCSA-FI[159] – Finnish National Cyber Security Centre, responsible for security matters related to the data transfer and handling of classified information in electronic communications. Among its main responsibilities, the NCSA-FI is responsible for the assessment and accreditation of information systems, assessment and approval of cryptographic products, as well as responsible of providing guidance on the secure handling of crypto material.

Regulatory Framework

In order to ensure the implementation of EU NIS Directive at national level, the Ministry of Transport and Communications established a working group on 4 October 2016.

National Laws:

7.11.2014/917 Law on securing electronic communications.

13.1.2015/10 Law on public administrations secure network activities.

28.6.2017/417 Law on the European Centre of Excellence for Countering Hybrid Threats.

Main Activities Performed

Based on VTT's study done in 2016 about cybersecurity competencies[160], Finland is home to some high-quality cyber security research, development and innovation activities and know-how. Strengths are found both in the business sector, as well as in universities and research institutions. However, the scope of Finland's cyber security know-how is relatively narrow, and there are relatively few top experts. In addition, this know-how is scattered across a vast number of organizations, and partnerships within the sector are not yet fully developed. Actions for ensuring national cybersecurity has been operational for 2017-2020.

[159] https://www.kyberturvallisuuskeskus.fi/en/our-activities/ncsa
[160] https://tietokayttoon.fi/documents/10616/2009122/9_Kyberosaaminen+Suomessa.pdf/29c8f675-0790-4c2f-91c2-69187b34b37e/9_Kyberosaaminen+Suomessa.pdf?version=1.0 (Only Finnish version available)

Impact Towards National Posture

The impact of the Finland actions towards national cybersecurity posture is threefold: (i) Improving international co-operation at EU-level and worldwide, (ii) Improving the coordination of cybersecurity management and preparedness. Several programs and a new post of national cyber security director back up this action; and (iii) Improving the national cybersecurity competence and expertise by investing on education at several levels and enhancing national cybersecurity related R&D activities.

Barriers and Challenges

The main identified challenges are (i) Evolving of cyber espionage and cybercrime worldwide, and (ii) Companies moving outside of Finland - knowledge leak and loss of control.

Identified needs and gaps

There are obvious knowledge gaps and shortages in a few areas of competence. International competition in the sector has also increased in recent years, and Finland needs to take decisive action to boost its cyber security competencies. Partnerships within the sector need to be deepened, and public procurement contracts, for example, used to increase know-how.

Identified initiatives

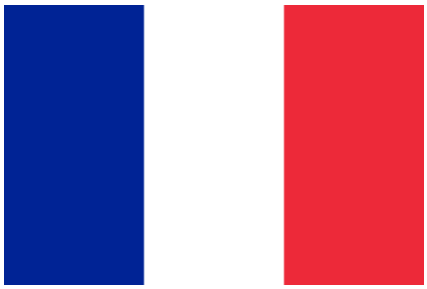
Finland has a National Cybersecurity Strategy[161], published initially in 2013 and lately updated in 2019. The initiative is funded by the Finnish Government and provides a vision of the cybersecurity in the country with strategic guidelines to be consider for improvement.

[161] https://valtioneuvosto.fi/delegate/file/61216 (Only Finnish version available, link to 2013 version in English) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/finlands-cyber-security-strategy

5.1.2 France

General Information

France has a National Cybersecurity Authority, namely ANSSI[162] – Agence Nationale de la Sécurité des Systèmes d'Information (National Cybersecurity Agency), aiming to fostering a coordinated, ambitious, pro-active response to cybersecurity issues in France. ANSSI has an annual budget of 100M€ and it is funded by the French administration.



Regulatory Framework

In the international context, The International Safety Management (ISM) Code has the following Key requirements:

- Commitment throughout the entire organization
- A safety environmental protection policy based on comprehensive risk assessment
- Procedures for normal operations and emergency situations
- A comprehensive methodology conducting audits and verifications
- A designated point of contact ashore to maintain a permanent link between ship and shore to check the safety management systems is being implemented
- A process for identifying gaps in practical implementation.

To address the specific cybersecurity risk, IMO has issued MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management providing high-level recommendations on maritime cyber risk management to safeguard shipping from cyber threats and vulnerabilities complementary to the safety and security management practices already established by the ISM Code.

The Maritime Safety Committee, at its 98th session in 2017, also adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems encouraging administrations to ensure that cyber risks are appropriately addressed in existing safety management systems.

The guidelines for preventing deliberate attacks on ships and port facilities is defined in the International Ship and Port Facility Security (ISPS)code applied to ships engaged on international voyages including passenger ships and cargo ships over 500 gross tonnage. The ISPS has been enforced in the European Union by EC regulation 725/2004.

EU implemented in addition a global cybersecurity framework on cybersecurity with:

- REGULATION (EU) 2019/881 OF THE EU PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the EU Agency for Cybersecurity) & on ICT cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[162] https://www.ssi.gouv.fr/en/

- REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC)

But the specificity of the maritime domain is provided mostly by classification agencies that have also implemented a regulatory but not mandatory framework.

Guidelines on Cyber Security on board Ships have been issued by BIMCO, Bureau Veritas, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, IUMI and WORLD SHIPPING COUNCIL.

Main Activities Performed:

The main activities carried out by ANSSI are the following:

- Reacting to the cyber threat
- Supporting product and services development.
- Providing information and advice.
- Training
- Accreditation.

Impact Towards National Posture

Since 2015, the agency deploys a territorial action mechanism which enables it to take direct action in the regions and tightly deal with local economic actors and authorities. In addition, the Global Cybersecurity Index [GCI18] places France in 2018 in second place in the Europe region, scoring 100 per cent in legal and organizational pillars. France is collaborating with institutional partners (ministries, national authorities, private sector and non-profit organizations) and, under the European cybersecurity month, using various means to raise cybersecurity awareness.

Barriers and Challenges

The challenge for improving efficient cybersecurity is collaboration. ENISA identified several challenges in that specific area, including lack of human resources and funding's, lack of trust between organizations, non-existence of legal basis for collaboration. Driving forces in the maritime sector have to be identified on identified issues having not necessary the same expectations for the different actors.

The maritime domain addresses several sectors (e-g. law enforcement, control, customs, environment, commercial activities deep into territories via riverine transportation, exploitation of maritime resources). Thrust building between entities has been initiated in this forum and opened to the overall maritime community around several initiatives (e.g. Naval Control) as well as for a maritime common information sharing environment promoted by the EUMSS and its reviewed action plan.

Identified needs and gaps

The outcomes of several past studies in the area of cybersecurity clearly raised the need for a legal settlement to avoid the fear to share and the need for common standards, semantics and processes implemented in interoperable cybersecurity solutions.

Identified initiatives:

The main cybersecurity initiative in France is the French national digital security strategy[163,164], announced on 2015 to support digital transition of French society. Today the technical answer needs to be coordinated allowing an identification of legal gaps and the definition of conditions for investigation and the coordination of response teams actions. Within the maritime community, public entities are initiating the first steps of a coordinated answer to the needs identified in support of technical solutions.

[163] https://www.ssi.gouv.fr/en/cybersecurity-in-france/
[164] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

5.1.3 Germany

General Information

Germany has a National Cybersecurity Authority, namely BSI[165] – Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security), which shapes information security in digitization through prevention, detection and reaction for government, business and society. The BSI has a budget of 163 M€ by (2020)[166], where the funds sources come from the national government and the EU.

Regulatory Framework

Since 2015, the issue of cyber security has been addressed by various legal acts in both German and European legislation. Cybersecurity is governed by several Acts in Germany[167]

- German IT Security Act (IT-SiG, 2015)
- German IT Security Act 2.0 (IT-SiG 2.0)
- The EU Directive 2016/1148 on Network and Information Security (NIS Directive, 2016)
- The EU Cybersecurity Regulation 2018/2019
- Collaboration with the ENISA

Main Activities Performed

The Federal Government aims to making a substantial contribution to a secure cyberspace, thus maintaining and promoting economic and social prosperity in Germany. The Cyber Security Strategy mainly focuses on civilian approaches and measures. They are complemented by measures taken by the armed forces to protect its capabilities and measures based on mandates to make cyber security a part of Germany's preventive security strategy. Germany works on following set of strategic priority areas:

- Protection of critical information infrastructures
- Secure IT systems in Germany
- Strengthening IT security in the public administration
- National Cyber Response Centre
- National Cyber Security Council
- Effective crime control also in cyberspace
- Effective coordinated action to ensure cyber security in Europe and worldwide
- Use of reliable and trustworthy information technology

[165] https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html
[166] https://www.bsi.bund.de/DE/Presse/BSI-Kurzprofil/kurzprofil_node.html
[167] http://intrapol.org/2019/06/25/overview-german-and-european-cybersecurity-regulation/

- Personnel development in federal authorities
- Tools to respond to cyber attacks
- Foster research & development

Impact Towards National Posture

With a strong defensive, technically and organizationally oriented approach, Germany has now achieved a high level of cybersecurity development. Following the US, Germany was one of the first countries with a far-reaching strategy to protect critical information infrastructures. Its implementation has been achieved through a mixture of a regulatory approach and a public-private partnership and is well underway compared to other European countries. Germany has also made reasonably rapid progress in setting up and legally enforcing the fight against cybercrime. The country has had a strong influence on European strategy and regulation in these two areas, protecting critical infrastructures and fighting cybercrime. Cybersecurity as an area of policy has attained high priority in Germany[168].

Barriers and Challenges

- Bilateral and multilateral cooperation among law enforcement agencies and with the private sector
- The lack of qualified personnel to implement the federal government's cybersecurity policies
- Balance between ensuring cybersecurity and national security and protecting civil liberties and privacy[169]

Identified needs and gaps

- Development of secure technologies,
- Dissemination of technical know-how,
- Technical and organizational security of critical systems,
- Legal obligation to and enforcement of protective measures,
- Development of defensive capabilities and increased criminal prosecution in the field of cybercrime.

Identified initiatives

There are several initiatives both nationwide and at the state level. Few worth mentioning are following:

- National Cybersecurity Strategy (NCSS)[170], aiming to presenting strategic objectives, measures and guidelines to implement the cybersecurity strategy in Germany.

[168] Schuetze J (2018) Warum dem Staat IT-Sicherheitsexpert:innen fehlen. Stiftung Neue Verantwortung, Berlin
[169] Schulze T (2006) Bedingt abwehrbereit. Schutz kritischer Informations-Infrastrukturen in Deutschland und den USA. VS Verlag, Wiesbaden

- Deutschland sicher im Netz[171], which provides wide range of information about security on the Internet and carries out projects to bring certain target groups to IT security, such as pupils, seniors, parents or users of certain Internet services.
- Initiative IT security in Business[172], with the primary goal of the cooperation between BMWi and business enterprises is to increase IT security in small and medium-sized enterprises.
- Initiative for Business Protection[173], to intensify cooperation between government and industry to protect German companies against industrial espionage, sabotage and other forms of crime

Additional Information

In Germany, the public and the private sector as well as society at large are all equally affected by targeted or coincidental IT failures.

[170] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en
[171] https://www.sicher-im-netz.de/sites/default/files/download/dsin-jahresbericht_2016_web.pdf.
[172] http://www.it-sicherheitin-der-wirtschaft.de/IT-Sicherheit/Navigation/root.html.
[173] Zedler D(2017) Zur strategischen Planung von cyber security in Deutschland. Zeitschrift für Außenund Sicherheitspolitik 10:67–85

5.1.4 Greece

General Information:

Greece has a National Cybersecurity Authority, namely Ministry of Digital Policy, Telecommunications and Media[174], responsible o the Greek National Cyber Security Strategy[175], with a budget of 5 M€ by (2019) coming mainly from the Greek government.

Regulatory Framework:

- Law 4577/2018: National implementation of NIS Directive (EU 2016/1148).
- Law 441/2016: National implementation of Directive EU 2013/40 and the Budapest convention on cybercrime
- Law 4624/2019: Clarifies certain national implementing measures regarding GPDR and incorporates the LED (Directive EU 2016/680).
- No 205/2013 Act of Hellenic Authority for Communication Security and Privacy (name also as "Regulation for the Security and Integrity of Networks and Electronic Communications Services")

Main Activities Performed:

- Development of a secure and resilient cyberspace that will be established according to national, EU and international rules, standards and best practices.
- Continuous improvement of capabilities which are necessary for protection against threats, and the development of a critical infrastructure for the safeguarding.
- Institutional shielding of the national cybersecurity framework that aims to reduce the effects of cyberattacks.
- Creation of a culture of security for citizens and the public and private sectors stakeholders

Impact Towards National Posture:

- Bridge the organizational and coordinative gap among the stakeholders involved in cyberspace security in Greece, both in the public and private sector.
- Evaluate, revise and update the National Cyber Security Strategy if required

Barriers and Challenges:

- Elements such as milestones or performance measures are not included in the National Cybersecurity Strategy and therefore it makes difficult for stakeholders to track the cybersecurity strategic plan in order to achieve stated goals and objectives.

[174] https://mindigital.gr/

[175] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/@@download_version/50cded9109d442e7839649f42055da60/file_en

- National Cybersecurity Strategy does not refer to the implementation of risk assessment analysis at national level which is followed by a scientific and technological process based on the identification, analysis and assessment of the effect of risk and it contributes to the creation of a plan for the protection of critical systems or networks or platforms per sector and/or per stakeholder.

Identified needs and gaps:

- Improvement of public awareness regarding cybersecurity
- Promotion of education and workforce planning and the increase of the efforts made by Research and Development (R&D)
- Assign roles and responsibilities related to international aspects of cybersecurity and collaborate among them at international level in order to address international cybersecurity challenges
- Knowledge on cyber threats could be enhanced if citizens are informed about the cyberattacks and malicious activities according to cyber security and their social impact. Therefore, educational campaigns both for the public and private sector stakeholders and citizens participating in the formulation of National Cybersecurity Strategy could strengthen cybersecurity at national level.

Identified initiatives:

Domain specific initiatives exist with a focus on ICT industry and mainly based on EU funded projects.

Additional Information:

- ENISA headquartered in Athens, Greece facilitates the cybersecurity national ecosystem awareness and technical expertise.
- Geopolitical situation in East Mediterranean broadens the attack surface/candidates to governmental/military targets resulting in increased interest on cybersecurity aspects.

5.1.5 Italy

General Information

Italy has a National Cybersecurity Authority, namely AgID176 – Agenzia per l'Italia Digitale (Digital Italy Agency), aiming to managing the implementation of the Italian Digital agenda's objectives, in coherence with the EU Digital Agenda by fostering innovation and economic growth. AgID has an annual budget of 220 M€ (by 2014) and its funded by the Italian government and the EU.

Regulatory Framework

All Cybersecurity related actions are regulated by the Cybersecurity Action Plan[177] - called "guidelines for cyberspace protection and IT national security", and the National cybersecurity framework[178] inspired on NIST.

Main Activities Performed

The activities performed by AgID focus on four main objectives: (i) Strengthening National Critical Infrastructures and other strategic players' defence capabilities; (ii) Improving cyber actors' technological, operational, and analytic capabilities; (iii) Encouraging public-private cooperation while Fostering cybersecurity culture; (iv) Reinforcing counter-action capabilities against online criminal activities.

The cybersecurity activities are designed to Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RE) from cybersecurity incidents.

Impact Towards National Posture

- Obtained a revised governance and improved responsibilities of the National Cybersecurity Management Board.
- Obtained a CERT's unification.
- Created a National Cryptographic Centre and a National Cybersecurity R&D Centre.
- The simplification of both ordinary and emergency management procedures has been reached.

[176] https://www.agid.gov.it/en
[177] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security/@@download_version/b267ff3c413e4dda9f82f58f1c00d44c/file_en
[178] https://www.cybersecurityframework.it/sites/default/files/CSR2015_ENG.pdf

Barriers and Challenges

The main challenges and barriers for this domain are the fact that there are too many actors and not enough coordination to execute all activities in this sector.

Identified needs and gaps

- Missing of a single cybersecurity crisis management system
- Need of a dedicated Command and Control structures capable of effective cyberspace military operations planning and implementation

Identified initiatives

Other identified initiatives in the cybersecurity domain are: The National Cybercrime Centre for the protection of critical infrastructures (CNAIPIC[179]), and the Joint Cybernetic Operations Command (CIOC[180]), with tasks in the areas of information security, computer network operations, cyber warfare, and cybersecurity.

[179] https://www.poliziadistato.it/articolo/10619
[180] https://en.wikipedia.org/wiki/Joint_Cybernetic_Operations_Command_(Italy)

5.1.6 Spain

General Information

Spain has a National Cybersecurity Authority, namely INCIBE[181] – Instituto Nacional de Ciberseguridad (Spanish National Cybersecurity Institute), and the CNPIC[182] - Centro Nacional de Protección de Infrestructuras y Ciberseguridad (National Centre of Infrastructure Protection and Cybersecurity).

INCIBE aims to improving digital trust, increasing cybersecurity and resilience, and contributing to the digital market while boosting the use of a secured cyberspace in Spain. CNPIC is more focused on the coordination and supervision of all policies and activities related to the Spanish critical infrastructure protection and cybersecurity.

Regulatory Framework

Law 36/2015 on National Security in Spain[183] defines the framework for crisis management at the national level.

Ministerial Order PRA/33/2018 regulates the functioning of the National Cybersecurity Council, as an expert advisory committee of the National Security Council.

Ministerial Order PRA/116/2017[184] announces an agreement on the implementation of mechanisms to guarantee the functioning of the National Security System, cybersecurity being part of this system [BSA15].

Main Activities Performed

User's protection and privacy, promoting mechanisms for the prevention and reaction to data security incidents, minimising their impact where they occur, and promoting advances in the culture of data security through training and the raising of awareness.

Impact Towards National Posture

Increase capabilities for the prevention, detection, investigation and response to cyber threats supported by an efficient and functioning legal framework.

Guarantee the security of information systems, communication networks and communication infrastructures common to all public administrations, reinforcing the safety of information systems that support critical infrastructures.

Improve the safety and resilience of ICT in the private sector by deploying state capabilities, while pushing actions directed towards strengthening the public-private partnership and the security of ICT systems employed by the industrial sector.

[181] https://www.incibe.es/en
[182] http://www.cnpic.es/
[183] https://www.global-regulation.com/translation/spain/615537/law-36-2015%252c-28-september%252c-national-security.html
[184] https://cms.law/en/INT/Publication/Data-Law-Navigator/Spain

Promote professional training in cyber security and boost the Spanish industry through a programme for research, development and innovation (RDI).

Develop a strong culture of cyber security, raising the awareness of citizens, professionals and companies of the importance of ICT security and the responsible use of new services in the knowledge society.

Enhance international cooperation for the creation of a safe and reliable cyberspace in collaboration with international initiatives, while safeguarding national interests at all times.

Barriers and Challenges

- Protecting cyberspace from the risks and threats hovering over it
- Appropriate coordination of the capabilities, resources and responsibilities involved in the national cybersecurity strategy
- Increase awareness on national cybersecurity strategy actions

Identified needs and gaps

According to a recent research [GLO19], the following needs and gaps are seen in the implementation of the cybersecurity measures in Spain:

- Sector-specific cybersecurity risk assessments have not been released.
- Lack of preparedness dominates the cybersecurity market in Spain.
- Shortage of cybersecurity experts

Identified initiatives

The Spanish National Cyber Security Strategy[185], approved in 2019, and aiming to addressing the different cybersecurity challenges with public-private cooperation and with support of a citizens aware of the changing reality and committed to the solutions of these challenges

Initiatives are designed and developed to meet the concrete needs of specific groups, namely: businesses and professionals who make use of ICTs; expertise in cybersecurity: through its team of cybersecurity specialists; and the general public.

European projects in Cybersecurity focusing on the generation of tools, or provision of services aligned with the strategic plan in Spain

Additional Information:

- Large Spanish defence & security firms' domination
- Economic regional disparities
- Rapid consolidation of market

[185] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

5.1.7 Sweden

General Information

Sweden has a National Cybersecurity Authority, namely Myndigheten för samhällsskydd och beredskap – MSB[186] (Swedish Civil Contingencies Agency), mainly responsible for issues concerning civil protection, public safety, emergency management and civil defence, before, during and after an emergency or crisis. In 2019, the MSB had an annual budget of SEK 1.2 billion (equivalent to 113.5M€).

Regulatory Framework

Today, provisions on information security are found in different regulatory frameworks:

Protecting the lives and health of the population, the functioning of society, and capacity to uphold fundamental values such as democracy, the rule of law and human rights and freedoms (Government Bill 2008/09:140, Committee Report 2008/09:FöU10, Riksdag Communication 2008/09:292).

IT policy objective – for Sweden to become the world leader in harnessing the opportunities of digital transformation (Government Bill 2011/12:1, Committee Report 2011/12:TU1, Riksdag Communication 2011/12:87).

National security strategy and in the digital strategy (N2017/03643/D).

Information security is one of three fundamental protective security areas under the Protective Security Act (1996:627). The legislation applies to the most security-sensitive activities in Sweden and entails far-reaching requirements for various protective measures.

Other central government authorities operate under the information security requirements set out in the Ordinance (2015:1052) on Emergency Preparedness and Surveillance Responsible Authorities' Measures at Heightened Alert.

Provisions on information security are also found in the Archives Act (1990:782), the Personal Data Act (1998:204) and the Electronic Communications Act (2003:389). In addition to these statutes, there are authority regulations governing information security in a number of sectors.

National strategy on the security of network and information systems.

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), began to be applied in May 2018 and entails higher requirements on the handling of personal data.

[186] https://www.msb.se/en/

Comprehensive cyber security action plan 2019–2022

Main Activities Performed

Activities related to cybersecurity consider the following ten objectives: (i) Address cybercrime; (ii) Balance security with privacy; (iii) Citizen's awareness; (iv) Critical Information Infrastructure Protection; (v) Develop national cyber contingency plans; (vi) Engage in international cooperation; (vii) Establish a public-private partnership; (viii) Establish an institutionalized form of cooperation between public agencies; (ix) Foster R&D; (x) Organize cyber security exercises.

Impact Towards National Posture

Conduct a systematic cyber security efforts by central government authorities, municipalities, county councils, companies and other organizations to have knowledge of threats and risks, assume responsibility for their cyber security and conduct systematic cyber security efforts.

- Create a national model to support systematic cyber security efforts.
- Enhance collaboration and cyber security information.
- Establish an appropriate supervision to create conditions for increasing society's cyber security.
- Promote electronic communications to be effective, secure and robust and in order to meet the needs of their users.
- Provide the needs of the supervisory authority's for being able to take adequate measures.
- Provide access to a secure data encryption system for IT and communications solutions based on society's needs.
- Promote security in industrial information and control systems.
- Enhance the capability to prevent, detect and manage cyberattacks and other IT incidents in society.
- Improve coordination between different stakeholders to manage cyberattacks and other serious IT incidents.
- Developed the cyber defence for the most security-sensitive activities in Sweden, with a strengthened military capability to meet and manage attacks from qualified opponents in cyberspace.
- Promote law enforcement authorities to have the preparedness and capability to combat cybercrime in an effective and appropriate manner.
- Increase the knowledge of individual digital technology users regarding the most urgent vulnerabilities and needs for security measures.
- Enhance Sweden's capability to manage the consequences of serious IT incidents by conducting both cross-sectoral and technical cyber security training.
- Enhance the International cooperation on cyber security.
- Promote the Cyber security as part of the ambition to safeguard free flows in support of innovation, competitiveness and societal development.

Barriers and Challenges

The scale of threats and risks in the area of information technology ranges from less extensive risks for private individuals is shifted to well-planned and precision attacks against vital parts of the functioning of society. According to the Swedish National Council for Crime Prevention (Brå), statistics show that crime with elements of IT (computer fraud, fraud committed with the aid of the internet, data infringement and internet-related child pornography crimes) increased by 949 per cent between 2006 and 2015 (2016:17).
Cyberattacks and various forms of intrusion in IT systems can constitute a separate antagonistic threat as well as one of several political and military instruments of power. The espionage and attacks from state and state-sponsored actors against security-sensitive activities in Sweden or against Swedish interests abroad is possible e.g. appropriating information about Swedish economic interests, Swedish companies, Swedish research, Swedish defence capability and planning, Sweden's security policy objectives, vital societal functions and critical infrastructure.
In addition, due to constant intrusion attempts against internet-connected systems, all those connected to the internet, both private individuals and private and public operations, are exposed to risks. Attacks can also be directed against the Sweden's fundamental values and the democratic functions of Swedish society, e.g. through disinformation and influence campaigns. Disinformation can be used to intentionally disseminate untrue or misleading details in order to influence people's attitudes, standpoints and actions in a certain direction. The number of cyberattacks aiming to influence the media is expected to increase.

Identified needs and gaps

In recent years, several inquiries and reviews in the area of cyber security have indicated deficiencies in relation to current threats and risks.

These include the Swedish National Audit Office's audits of information security in public administration (RIR 2016:8, RIR 2014:23). The report Cyber security in Sweden also contains several proposals in the area of cyber security (SOU 2015:23). In its defence policy bill, the Government assessed that Sweden's overall capability to prevent, counteract and actively manage consequences of civil and military threats, events and attacks in the cyber environment must be developed and strengthened (Government Bill 2014/15:109).

To protect the country the responsibility must be shared by all of society and be conducted both by the Government and in the activities of municipalities, county councils, authorities, companies and organizations in Sweden. Systematic cyber security efforts are necessary for enabling stakeholders in society to maintain a well-balanced level of cyber security.

Technical security needs to be further enhanced while taking into account the fact that in many cases it is the human factor that is behind incidents or is exploited during attacks. For this reason, it is important to raise the awareness and ability of all users of IT systems and to create conditions for developing a security culture throughout society.

To reduce vulnerabilities and to promote the objectives of Sweden's security and IT policy, it is the Government's assessment that society's cyber security efforts above all need to priorities;

- Securing a systematic and comprehensive approach in cyber security efforts;
- Enhancing network, product and system security;
- Enhancing capability to prevent, detect and manage cyberattacks and other IT incidents;
- Increasing the possibility of preventing and combating cybercrime;

- Increasing knowledge and promoting expertise;
- Enhancing international cooperation;

There are a number of extensive areas that the authorities deemed to be of major significance to strengthening cyber security in society but were not fully handled within the measures in the 2019 edition of the action plan due to insufficient resources or mandates.

Identified initiatives

The main cybersecurity initiative is the Swedish National Cyber Security Strategy[187], implemented in 2017, aiming to helping to create the long-term conditions for all stakeholders in society to work effectively on cyber security, and raise the level of awareness and knowledge throughout society.

National Cyber Security Authorities include: (i) National Defence Radio Establishment | Signals Intelligence and cyber security services; (ii) Swedish Police Authority; and (iii) Swedish Post- and Telecom Authority | Security in electronic communications.

National Cyber Security Agencies include: (i) Swedish Armed forces; (ii) Swedish Civil contingencies Agency | Supporting and coordinating work with societal information security; (iii) Swedish Defence Materiel Administration | Swedish Certification Body for IT Security; and (iv) Swedish Security Service.

National Information Sharing and Analysis Centres (ISACs) include: (i) Elsamverkan; (ii) FIDI-FINANS, (iii) FIDI-SCADA; (iv) FIDI-TELEKOM; (v) FSPOS; (vi) National Telecommunications Co-ordination Group; (vii) TP SAMS; (viii) Swedish Armed forces; and (ix) Swedish Police Authority.

Public Private Partnerships (PPPs) includes the National Telecommunications Co-ordination Group.

Additional Information

There are several good examples of collaboration in the area of cyber security in Sweden.

The Cooperation Group for Information Security (SAMFI) plays an important role through its work for secure information assets in the society. SAMFI consists of a number of central government authorities that have particular tasks in the area of cyber security:

- The Swedish Civil Contingencies Agency (MSB),
- The Swedish Defence Materiel Administration,
- The National Defence Radio Establishment (FRA),
- The Swedish Armed Forces,
- The Swedish Police Authority,
- The Swedish Post and Telecom Authority (PTS); and
- The Swedish Security Service.

[187] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/swedish-national-cyber-security-strategy/@@download_version/d8934f793fe048d09804a9f17c41d13b/file_en

The MSB has administrative responsibility for the group. The collaborative forum, the National Cooperative Council against Serious IT Threats (NSIT), analyses and assesses threats and vulnerabilities regarding serious or qualified cyberattacks against the most security-sensitive national interests. NSIT consists of the Swedish Security Service, FRA and the Swedish Armed Forces through its Military Intelligence and Security Service (MUST).

5.1.8 United Kingdom

General Information

The U.K. has a National Cybersecurity Authority, namely NCSC[188] – National Cyber Security Centre, responsible of providing effective incident response to minimize harm to the UK, help with recovery, and learn lessons for the future. The NCSC has a budget of £1.9 billion (2016 – 2021), funded by the United Kingdom Government.

Regulatory Framework

The National Cyber Security Centre (NCSC) operates within the general cyber security regulatory environment in the United Kingdom (UK) which includes both the Network and Information Systems Regulations 2018 (NIS) and the General Data Protection Regulation (GDPR).

NIS implements the European Directive 2016/1148 on a high common level of security of network and information systems across the Union, also known as the 'NIS Directive'.

Main Activities Performed

The National Cyber Security Centre aims to support the most the most critical organizations in the UK, the wider public sector, industry, SMEs and well as the general public.

The main activities of the NCSC include:

- Assisting in the development of cyber security standards and guidance (such as the CAF collection)
- Supporting, encouraging and facilitating cyber security research and innovation within the UK.
- Responding to cyber security incidents to reduce the harm they cause to organizations
- Use industry and academic expertise to nurture the UK's cyber security capability.
- Reducing risks to the UK by securing public and private sector networks.

[188] https://www.ncsc.gov.uk/

In the United Kingdom, the National Cyber Security Centre provides a single point of contact for SMEs, larger organizations, government agencies, the general public and departments. We also work collaboratively with other law enforcement, defence, the UK's intelligence and security agencies and international partners.

The National Cyber Security Centre also develops and maintains the Cyber Assessment Framework (CAF) collection which is a cyber assessment framework intended for use by organizations that are responsible for services and activities that are of critical importance.

Impact Towards National Posture

The NCSC is continually undertaking activities that aim to improve the cybersecurity landscape in the UK and improving the UK's cyber-security posture. This has included the implementation of numerous projects such as the NCSC assists local government both through direct engagement at a local level, supporting its networks of technical staff, and working with representatives from member organizations including the Local Government Association (LGA) and the Society of Local Authority Chief Executives (SOLACE).

The NCSC runs a Vulnerability Reporting Service. This is part of its wider efforts to improve vulnerability handling across the public sector. Following the service's launch, the NCSC has received reports covering a number of security issues including cross-site scripting and subdomain takeover. In addition to the Reporting Service, the NCSC also launched the Vulnerability Disclosure Pilot, working with a number of UK government departments to kick start best practice in vulnerability disclosure across the public sector.

NCSC's pioneering Haulster operation has disrupted financial cybercrime by flagging fraudulent intention against more than one million stolen credit cards. It is in the process of scaling this operation and hope to reduce considerably more attacks in the near future.

The Border Gateway Protocol (BGP) is used to route the internet between Internet Service Providers (ISPs) around the world. When BGP is misused, either accidentally or maliciously, it can disrupt the internet until the issue is resolved. The NCSC has built BGP Spotlight, a detection and analysis system for BGP, that will alert the UK's carriers when BGP misuse occurs to allow them to respond quickly, analyze the cause, and minimise disruption to the UK's internet

Barriers and Challenges

The rapid implementation of connectivity in industrial control processes in critical systems, across a wide range of industries such as energy, mining, agriculture and aviation, has created the Industrial Internet of Things. This is simultaneously opening up the possibility of devices and processes, which were never vulnerable to such interference in the past, being hacked and tampered with, with potentially disastrous consequences.

Poor cyber hygiene and compliance. Awareness of technical vulnerabilities in software and networks, and the need for cyber hygiene in the UK, has undoubtedly increased over the past five years but still remains a key challenge.

The ready availability of hacking information and user-friendly hacking tools on the Internet is enabling those who want to develop a hacking capability to do so. The information hackers need in order to compromise victims successfully is often openly accessible and can be harvested quickly.

Legacy and unpatched systems. Many organizations in the UK will continue to use vulnerable legacy systems until their next IT upgrade. Software on these systems will often rely on older, unpatched versions. These older versions often suffer from vulnerabilities that attackers look for and have the tools to exploit. An additional issue is the use by some organizations of unsupported software, for which patching regimes do not exist.

Identified needs and gaps

Insufficient training and skills. There is a lack the skills and knowledge to meet our cyber security needs across both the public and private sector. In businesses, many staff members are not cyber security aware and do not understand their responsibilities in this regard, partially due to a lack of formal training. The public is also insufficiently cyber aware.

Identified initiatives

The main initiative is the National Cyber Security Strategy[189] (2016 to 2021), aiming to defining the national roles and responsibilities towards all cybersecurity related aspects.

5.1.9 Cybersecurity Ecosystem Main Findings

Table 12 presents a summary of the main cybersecurity aspects found in the eight European countries that participated in the study.

Table 12. Cybersecurity Ecosystem in Europe Main Findings

Finland	France	Germany	Greece
			
- Cybersecurity scope is relatively narrow, with few top experts. - Partnerships within	- Solid regulatory framework, including maritime cybersecurity management	- Achieved high level of cybersecurity development - Rapid progress in setting up and	- Missing elements in the National Cybersecurity Strategy that makes difficult to track the

[189] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

the sector are not yet fully developed. - Strength is found in the business sector, universities and research institutions.	- Collaboration with institutional partners to raise cybersecurity awareness - Need for common standards, semantics and processes implemented in interoperable cybersecurity solutions. - Need for a legal settlement to avoid the fear to share.	legally enforcing the fight against cybercrime - Lack of qualified personnel to implement the federal government's cybersecurity policies - Missing bilateral and multilateral cooperation among law enforcement agencies and with the private sector	cybersecurity strategic plan to achieve goals. - Lack of risk assessment analysis at national level - Need of a plan for the protection of critical systems or networks or platforms per sector and/or per stakeholder. - Clear gap on the improvement of public awareness regarding cybersecurity
Italy	**Spain**	**Sweden**	**United Kingdom**
			
- Too many actors and not enough coordination to execute all activities in this sector - Missing of a single cybersecurity crisis management system - Need of a dedicated Command and Control structures capable of effective cyberspace military operations planning and implementation	- Lack of preparedness dominates the cybersecurity market - Sector-specific cybersecurity risk assessments have not been released - Shortage of cybersecurity experts - Large Spanish defence & security firms' domination - Economic regional disparities	- Cybercrime substantially increased during the last decade and it is expected to continue increasing - Capabilities to prevent, counteract and actively manage consequences of civil and military threats, events and attacks in the cyber environment need to be developed and strengthened - Good national collaboration but low international cooperation	- Use industry and academic expertise to nurture its cyber security capabilities - Work collaboratively with national and international partners - Lack of skills and knowledge to meet cyber security needs across public and private sectors. - Poor cyber hygiene and compliance. - Awareness of technical vulnerabilities in software and networks increased over the past years but still remains a key challenge.

5.2 Maritime Ecosystem

5.2.1 Finland

Identified initiatives

The Sea for Value – Fairway DIMECC[190] program is the first program initiative under the One Sea ecosystem[191].

Other national initiatives are: The National emergency Supply Agency[192] with a focus on an executive maritime business platform[193]; and the Finnish Marine Industries' platform for publications[194].

Regulatory Framework

Government Resolution on Finland's maritime policy guidelines: from the Baltic Sea to the oceans[195]. The policy guidelines determine the focus areas of Finland's maritime policy concerning oceans and seas, and present measures required for reaching the set objectives.

Stricter provisions on sulphur emissions from shipping entered into force at the beginning of 2015. (Regulations: International Maritime Organization (IMO) and EU Sulphur Directive.) Ships can meet with the new provisions by using low-sulphur fuel, installing scrubbers or shifting to the use of alternative fuels, such as liquefied natural gas (LNG).

Main Activities Performed

Jaakonmeri test area[196] located in coastal area of Finland, which can be used to test and validate autonomy related maritime technology for surface vessels in authentic and challenging sea conditions (incl. arctic). The test area is open to all organizations and companies. Jaakonmeri test area is operated by DIMECC Ltd, a leading high-tech co-creation ecosystem that speeds up time to market.

Impact Towards National Posture

One Sea is a high-profile ecosystem with a primary aim to lead the way towards an operating autonomous maritime ecosystem by 2025.

[190] https://www.dimecc.com/dimecc-services/s4v/
[191] https://www.oneseaecosystem.net/
[192] https://www.nesa.fi/organisation/the-national-emergency-supply-agency/
[193] https://www.seafocus.fi/national-emergency-supply-agency
[194] https://meriteollisuus.teknologiateollisuus.fi/en/association/finnish-marine-industries-publications
[195] http://julkaisut.valtioneuvosto.fi/handle/10024/161376
[196] https://www.oneseaecosystem.net/test-area/

Barriers and Challenges

Finland has relatively large number of cargo ports which are all different in ownership, size, location, clients and physical/ICT system infrastructure. The increased digitalization trend in the maritime logistics will create challenges for the Finnish ports in order to have up-to-date systems and interfaces in addition to efficient cybersecurity protocols.

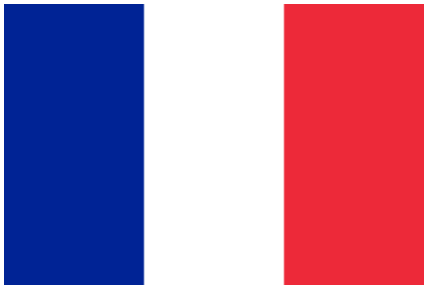
Identified needs and gaps

There are various stakeholders operating in the Finnish ports and the ICT-infrastructure is quite unstructured. There has been discussion and preliminary projects in in order to have Port Community Systems / PCS type of arrangements to the main cargo ports of Finland.

There are no cybersecurity standards presently within Finnish maritime domain and the recent empirical research has indicated a lack of cybersecurity preparedness and awareness.

5.2.2 France

Identified initiatives



The maritime domain has developed several initiatives and developed in France an original approach under the head of the secretary for the sea (SGMER) that federates the public organizations operating at sea (e-g. law enforcement, control, customs, environment, commercial activities..) and powerful maritime federations representing more than 700 entities. Thrust building between public and private entities has been initiated around several initiatives (maritime information coordination and awareness centre) as well as a shared governance structure in 2019. To furthermore develop a common approach in the domain an ambitious project of Maritime Cybersecurity Coordination Centre foresees to support the digital transformation of Europe's Maritime sector[197].

Regulatory Framework

Military Programming Law - Loi de Programmation Militaire (LPM) and other national regulations for Critical Infrastructure. With the NIS directive, it is the operators of essential services (OES) of economic sectors that are targeted to protect their activity from cyber-risks. Since 2018, the NIS Directive is implemented by Member States. Maritime industry is one of the sectors affected, though.

Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security[198] (Document 02004R0725-20090420)

The International Ship and Port Facility (ISPS[199]) Code, IMO. The ISPS code is derived in European law (c.f. above) and then in domestic laws for European country.

Main Activities Performed

SGMER (Secretariat Général à la Mer, under French Prime Minister) is in charge of a global cybersecurity strategy for the maritime domain including ships and harbours. In particular, a Maritime CERT (so-called M-CERT) is under creation. As a first step, its perimeter is national and as a second step European perimeter will be addressed.

Impact Towards National Posture

The military cybersecurity law - LMP (2019 - 2025) has already introduced a "criminal excuse for cyber combatants" operating in the digital world. The Military Cyber-Defence Command

[197] http://www.imo.org/fr/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx
[198] https://eur-lex.europa.eu/eli/reg/2004/725/2009-04-20
[199] http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/solas-xi-2%20isps%20code.aspx

(COMCYBER) wants to be able to conduct offensive cyber operations without legal risks such as infiltration, collection of information or counterpropaganda in the context of terrorist activities. The objective to extend the current framework to “influence operations" are envisaged as well as "coercion measures” on adversaries in order to persuade them or to force them to stop their activities. With this “criminal excuse” there is the will to avoid any legal coercive response.

Barriers and Challenges

In terms of digital vulnerability of ships, until now only terrestrial, maritime and port infrastructures seem concerned. In 2011, the port of Anvers detected an anomaly in its container management system. The investigation concluded to “cyber-concealing” of several containers from South America.

Ships are a means of transport amongst many other, long known as being apart from the web connections. However, they seem not to be totally out of the “triangle of motivation” of the cyber threat: money theft, sensitive data theft, activism/ terrorist acts [FRC16].

Identified needs and gaps

Numerous small and medium enterprises (SME’s) are connected to maritime systems and installations (logistics, dockers, shipbuilding actors). SME’s contribution to the maritime sector is high, even though limited security capacities. The consequences of inappropriate security considerations can be disastrous for all the sector during their interactions with the main stakeholder. Involved (as active of passive element) in the different activities, SME’s contribute with their strengths and weaknesses to the establishment of a global cybersecurity picture and their risks as the lowest common multiple elements of the cybersecurity need.

5.2.3 Germany

Identified initiatives

The following initiatives have been identified in Germany for the maritime domain:

- Maritime Agenda 2025[200], "The future of Germany as a maritime industry hub". Approved on 11 January 2017 by the Federal Cabinet; developed jointly by several different ministries; focusing on the time until 2025; long-term framework that will make it possible to shape the future of the maritime industry in a targeted manner and strengthen Germany's role as a maritime hub.

- The "Maritime security" call - Projects in the "Maritime security" field[201]:
  (i) EMSec: Real-time services for maritime security[202]
  (ii) MAR-SIMNET: Maritime simulator network[203]
  (iii) OWISS: Offshore wind energy – Protection and security[204]
  (iv) SIREVA: Passenger security in rescue and evacuation from vessels[205]

- Maritime Safety[206], a permanent task and objective of the Federal Ministry of Transport and Digital Infrastructure (BMVI) in the International Maritime Organization and the European Union.

- National Master Plan for Maritime Technologies[207]

Regulatory Framework

Maritime Labour Act (SeeArbG) of 20 April 2013 (Federal Law Gazette [BGBl.] Part I p. 868), last amended by Article 1 of the Act of 22 December 2015 (BGBl. Part I p. 2569)[208]

Regulations on the Competencies and Proficiencies of Seafarers in the Maritime Shipping industry (Seafarers' Competencies and Proficiencies Regulations; See-BV) of 8 May 2014 (Federal Law Gazette [BGBl.] Part I p. 460), last amended by Article 66 of the Act of 2 June 2016 (Federal Law Gazette I p. 1257)[209]

Ordinance on the Licensing of Security Companies on Ocean-Going Vessels (Seeschiffbewachungsverordnung - SeeBewachV) - not only legalized and organized the employment of Private Maritime Security Companies (PMSC) but constitutes a clear legal

[200] https://www.bmwi.de/Redaktion/EN/Publikationen/maritime-agenda-2025.html
[201] https://www.sifo.de/en/approved-projects-in-the-maritime-security-field-2149.html
[202] https://www.sifo.de/de/emsec-echtzeitdienste-fuer-die-maritime-sicherheit-2119.html
[203] https://www.sifo.de/de/mar-simnet-maritimes-simulatornetzwerk-2346.html
[204] https://www.sifo.de/de/owiss-offshore-windenergie---schutz-und-sicherheit-2383.html
[205] https://www.sifo.de/de/sireva-sicherheit-von-personen-bei-rettungs-und-evakuierungsprozessen-von-2347.html
[206] https://www.bmvi.de/EN/Topics/Mobility/Water/Maritime-Safety/maritime-safety.html
[207] https://www.nmmt.de/
[208] https://www.gesetze-im-internet.de/englisch_seearbg/index.html
[209] http://www.gesetze-im-internet.de/englisch_see-bv/

framework and represents the first high quality standard for private security services on board of German flagged vessels.[210]

Implementing Ordinance for the Ocean-Going Vessel Security Ordinance (Seeschiffbewachungsdurchführungsverordnung - SeeBewachDV)[211]

Regulation on fees and expenses (Seeschiffbewachungs-gebührenverordnung – SeeBewachGebV)[212]

Trade Regulation Code (Gewerbeordnung - § 31 Bewachungs-gewerbe auf Seeschiffen)[213]

Weapons Act (WaffG) - Section 28a: Acquisition, possession and carrying of guns or ammunition by security operators and their personnel for security tasks pursuant to Section 31 (1) of the Trade Regulation Code.[214]

Ordinance on verification of compliance of working and living conditions on board ships - Maritime Working Verification Ordinance of 25 July 2013 (Federal Law Gazette [BGBl.] Part I p. 2800)[215]

Ordinance on the table of shipboard working arrangements and records of hours of work in maritime shipping (See-Arbeitszeitnachweisverordnung - See-ArbZNV)[216]

Ordinance Pursuant to Vocational Training in Maritime Shipping (Maritime Vocational Training Ordinance - See-BAV)[217]

Ordinance on Accommodation and Recreational Facilities for Crew Members on Board of Merchant Vessels (Ordinance on Accommodation in Maritime Shipping – MaritimeAccommodationO, SeeUnterkunftsV)[218]

Main Activities Performed

Means to implement the Maritime Agenda[219] 2025:

- Maritime coordination, intercommunication and dialogue forums
- Developing the National Master Plan for Maritime Technologies
- Promoting research, development and innovation on the sustainable use of the seas
- National Port Concept for Sea and Inland Ports
- Securing Germany's economic prospects as a shipping location, efficient maritime transport
- Maritime Safety
- Promotion of foreign trade and investment
- Training and employment

[210] http://www.gesetze-im-internet.de/seebewachv/
[211] http://www.gesetze-im-internet.de/seebewachdv/
[212] http://www.gesetze-im-internet.de/seebewachgebv/
[213] https://www.gesetze-im-internet.de/gewo/__31.html
[214] http://www.gesetze-im-internet.de/englisch_waffg/englisch_waffg.html#p0313
[215] http://www.gesetze-im-internet.de/englisch_seearb_v/index.html
[216] http://www.gesetze-im-internet.de/englisch_see-arbznv/index.html
[217] http://www.gesetze-im-internet.de/englisch_see-bav/index.html
[218] http://www.gesetze-im-internet.de/englisch_seeunterkunftsv/index.html
[219] https://www.bmwi.de/Redaktion/EN/Publikationen/maritime-agenda-2025.html

- Climate and environmental protection in the maritime industry
- Public procurement

Other measures employed by the Federal Ministry for Economic Affairs and Energy to provide support for the maritime industry[220]:

- 2025 maritime research strategy - provides funding for research and development and covers the entire spectrum of ship, production, shipping and maritime technology. From 2011 to 2017, the Economic Affairs Ministry provided €225 million in funding for 485 maritime R&D projects.
- Promoting sustainability in shipping - cross-programme funding initiative "Energy transition in transport", with total funding of €130 million.
- Improving German companies' capacity to export - Fixed-rate financing at the CIRR rate and export credit guarantees from the Federal Government ensure that German companies can operate on a level playing field.
- Dialogue with the maritime industry - prompting close dialogue between policymakers and the business sector; National Master Plan for Maritime Technologies (NMMT) as a key tool for coordination and networking.
- Keeping shipping routes safe - a mechanism for the licensing of private-sector security companies was launched in 2013 in order to help protect the crews against piracy and armed robbery attacks and in order to offer legal certainty to the shipping lines and security firms.
- LeaderSHIP strategy - dialogue between the Federal Ministry for Economic Affairs and Energy and the shipbuilding industry, which allows all the stakeholders to discuss priorities for research and working methods.
- The Maritime Conferences - are held every two years and are a good opportunity for the Federal Ministry of Economic Affairs and Energy to join with all the relevant stakeholders to devise measures that help strengthen Germany's position as a maritime hub.

Impact Towards National Posture

The maritime industry is one of the most important sectors of the German economy. The sector is not just limited to the key sites on the North Sea and Baltic Sea coasts - maritime production takes place all over Germany: supply companies are based in all regions of Germany, in particular in Baden-Wuerttemberg, Bavaria and North Rhine-Westphalia.[221]

More than other sectors, Germany's maritime industry is closely connected to the global economy and global sea trade. In comparison to other sectors of the economy, this makes the industry particularly vulnerable to global economic changes and fluctuations.

Germany is a country that is very much oriented towards foreign trade. A strong and internationally competitive maritime sector is therefore of great importance for the entire economy as it drives Germany's competitiveness and helps safeguard growth and employment. The business community and policymakers seek to ensure that the maritime industry is structurally strong and that it can harness its full potential. Estimates place the annual turnover at up to €50 billion and the number of jobs which are directly or indirectly dependent on the

[220] https://www.bmwi.de/Redaktion/EN/Dossier/maritime-industry.html
[221] https://www.bmwi.de/Redaktion/EN/Publikationen/maritime-agenda-2025.html

maritime industry at up to 400,000. This makes it one of the most important sectors of the German economy.

The industry is characterised by its modern, high-tech shipbuilding and shipbuilding supply industries, its globally leading shipping companies, its high-performance port and logistics industries, its innovative marine engineering industry, and its renowned maritime research and training facilities. The German government seeks to adopt an integrated policy approach that helps safeguard jobs, economic output and training and thus strengthen the German maritime industry as a whole.[222]

Barriers and Challenges

Increasing digitalisation of maritime logistics chains (automation and digitalisation of products and services, production and logistic processes)

Meeting the objective of environmental and climate protection and nature conservation in the shipping industry (increasing environmental and climate standards)

Demand for skilled labour and demographic change

The maritime industry faces tough international competition on global markets - German shipyards compete internationally with state funded companies that distort fair competition for shipbuilding contracts. German shipping companies are also experiencing growing competitive pressure, which is exacerbated by severe excess capacity in the transport sector and low charter rates and freight rates. Also facing stiff international competition are the German ports.[223]

Maritime security is of particular importance for industrial value chains. The organization and execution of many maritime activities are subject to complex safety and security provisions, which require technical surveillance and monitoring systems in order to ensure a high level of safety and security and to minimise risks. This means that the maritime safety and security partnership between state authorities and the concerned companies must constantly evolve. The challenges will continue to grow as a result of pressure to reduce costs, increasing traffic volumes, in part with increasingly large container ships, and also in terms of the expansion, operation and maintenance of offshore wind parks and the continually high growth rates in cruise tourism and in recreational boating. Increased requirements for responsible emergency preparedness must be satisfied using state-of-the-art equipment and highly qualified personnel.[224]

The maritime industry is directly affected quite unlike any other sector by developments on international markets and the trade and subsidy policies of other countries. Whilst EU state aid law provides clear and reliable provisions for state subsidies, in other economic areas there is a recognisable trend towards stronger state subsidies, particularly subsidies that favour the own maritime industry, for instance shipyards. This leads to international market distortions, which are detrimental to all market operators in the end.[225]

[222] https://www.bmwi.de/Redaktion/EN/Dossier/maritime-industry.html
[223] https://www.bmwi.de/Redaktion/EN/Publikationen/maritime-agenda-2025.html
[224] https://www.bmwi.de/Redaktion/EN/Publikationen/maritime-agenda-2025.html
[225] https://www.bmwi.de/Redaktion/EN/Publikationen/maritime-agenda-2025.html

A growing trend of maritime ports (and port infrastructure) privatisation has been observed (e.g. port of Hamburg). This privatisation trend raises several justified concerns regarding the security requirements set for ICT implementations and use in ports, as the security baselines and standards put in place may not necessarily depend on the port's country of origin, but rather on the current owner. It additionally brings forwards additional security challenges due to the international dimension, as the actual owners can originate from outside of the EU borders.[226]

Another key issue concerns the critical ICT components developed and implemented by the large variety of international vendors that provide services and infrastructure to the ports, and to the maritime sector in general. As development and testing cycles are increasingly being managed to lower costs countries (typically outside European Member States), a series of vulnerabilities are left exposed (e.g. missing patches, IT breaches).[227]

Identified needs and gaps

In the current regulatory context for the maritime sector on global, regional and national levels, there is **very little consideration given to cyber security elements**. Most security related regulation only includes provisions relating to safety and physical security concepts, as can be found in the International Ship and Port Facility Security (ISPS) Code and other relevant maritime security and safety regulations, such as Regulation (EC) No 725/2004 on enhancing ship and port facility security. These regulations do not consider cyber-attacks as possible threats of unlawful acts.[228]

Most of the world's largest ports have only limited cyber security strategies or cyber incident response plans in place, while the involved organizations have yet to establish company-wide cyber risk awareness programs.[229]

Maritime Agenda 2025 - Federal Government areas of action and maritime industry policy objectives:[230]

- Consolidate and expand technological leadership
- Strengthen international competitiveness
- Consolidate competitiveness of German ports, expand infrastructure and secure Germany's leading position as a logistics hub
- Shape maritime transport sustainability – strengthen climate and environmental protection and nature conservation
- Contribute to the energy transition using maritime technologies
- Maritime 4.0 – use the opportunities of digitalisation
- Strengthen Germany's maritime expertise
- Develop industrial capabilities in naval and coastguard shipbuilding
- Play an active role in shaping the EU's Blue Growth Strategy

[226] https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1
[227] https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1
[228] https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1
[229] https://elib.dlr.de/98812/1/Look-Out%202016_web.pdf
[230] https://www.bmwi.de/Redaktion/EN/Publikationen/maritime-agenda-2025.html

5.2.4 Greece

Identified initiatives:

Greek Maritime Cluster – Maritime Hellas[231]: On the initiative of the Hellenic Chamber of Shipping (NEE), the Union of Greek Shipowners (UGS) and the Piraeus Chamber of Commerce and Industry (PCCI), the internet site of the Greek Maritime Cluster, entitled "Maritime Hellas navigate the Greek Cluster", was established.

Regulatory Framework:

The Code of Private Maritime Law (CPML) regulates private shipping law matters in Greece (such as crew claims, collisions, salvage and time bars). In parallel, the Code of Public Maritime Law regulates public shipping law matters (such as ship registries, the obligations of vessel masters and the duties of pilots). Numerous presidential decrees and ministerial decisions regulate specific maritime issues, such as Greek ports.

i Safety

Greece applies all EU and IMO regulations and international conventions relating to safety at sea. The most important are:

- the Convention on the International Regulations for Preventing Collisions at Sea, 1972 (COLREGs);
- the International Convention for the Safety of Life at Sea (SOLAS) and all its protocols and amendments;
- the International Management Code for the Safe Operation of Ships and for Pollution Prevention (ISM Code); and
- EU Regulation No. 1406/2002 establishing a European Maritime Safety Agency as amended by EU Regulation No. 1625/2016.

ii Port state control

Greece is a member of the Paris Memorandum of Understanding (MOU) and has implemented the port state control regime. The guidelines of the Paris MOU apply to all ships calling at Greek ports and anchorages, irrespective of their flags.

During 2017, 1,016 inspections were carried out, 567 deficiencies were recorded, and 66 detentions were ordered.

iii Registration and classification

All major Greek ports have their own ship registries, kept by the local port authorities. The vast majority of ships under the Greek flag are registered in the port of Piraeus.

[231] https://www.maritimehellas.org

To be registered in a Greek ship registry (i.e., under the Greek flag), a ship must be more than 50 per cent beneficially owned by Greek or other EU nationals. Various documents are required for the registration of a ship in a Greek registry.

The following classification societies are approved to issue certificates in respect of Greek-flagged vessels:

- the American Bureau of Shipping;
- Bureau Veritas;
- the China Classification Society;
- DNV GL;
- Lloyd's Register;
- the Korean Register of Shipping;
- Class NK (Nippon Kaiji Kyokai);
- Registro Italiano Navale (RINA);
- the Russian Register of Shipping;
- the Hellenic Register of Shipping;
- the International Naval Survey Bureau; and
- the Phoenix Register of Shipping.

Classification societies can be held liable to the owners of the ships they monitor if they have breached their contractual obligations to them. They can also be held liable in tort to third parties if they have acted negligently in the performance of their duties and that negligence caused loss or damage to the third party (e.g., seafarers who suffer injuries because of the ship's defects).

The classification society that monitored a vessel before its sale can be held liable to the buyers of the vessel under Greek consumer protection laws if it has erroneously described the vessel's condition in her class records.

iv Environmental regulation

Greece has ratified the International Convention for the Prevention of Pollution from Ships 1973 (MARPOL), as modified by the Protocol of 1978, and the Annexes thereto: Annex I (Prevention of Pollution by Oil), Annex II (Control of Pollution by Noxious Liquid Substances), Annex III (Prevention of Pollution by Harmful Substances in Packaged Form), Annex IV (Prevention of Pollution by Sewage from Ships), Annex V (Prevention of Pollution by Garbage from Ships) and Annex VI (Prevention of Air Pollution from Ships).

The following conventions have also been ratified by Greece:

- the CLC Convention;
- the London Dumping Convention;
- the Convention for the Protection of the Mediterranean Sea Against Pollution;
- the OPRC Convention; and
- the Bunker Convention.

v Collisions, salvage and wrecks

Greece has ratified the Collision Convention and the Salvage Convention. Issues relating to wreck removal are governed by Greek law, the Greek State not having yet ratified the Nairobi

Convention. The owner of a wreck that endangers other vessels (in ports, canals or channels) is obliged to remove the wreck at its own expense, otherwise the authorities are entitled to remove it at the owner's expense. There is no specific regulation on the recycling of shipwrecks.

To the extent that no Lloyd's Open Forum or other agreement with a foreign jurisdiction clause is signed between the salvor and the owner of a salvaged vessel, salvage cases relating to incidents that take place in Greece are litigated before the Greek courts. The amounts awarded to salvors by the Greek courts are generally considered to be less generous than those awarded in London arbitration.

The conditions for a salvage claim under Greek law are as follows:

- assistance is offered to a vessel;
- the vessel receiving assistance faces a danger of loss or of sustaining damage. This danger must be real, even if not imminent, but predictable, possible and existing at the time of the offering of salvage services. The existence and extent of the danger are examined by reference to all the facts and circumstances surrounding the particular incident; and
- the salvors' actions must have a beneficial result.

vi Passengers' rights

Greece has ratified the Athens Convention and the subsequent 2002 Protocol. The Athens Convention applies to international carriages when the place of departure and the place of destination are located in two different states, or in a single state if, according to the contract of carriage or the scheduled itinerary, there is an intermediate port of call in another state. Following the introduction of the EU Passenger Liability Regulation 2009 (PLR), the Athens Convention also applies to domestic carriages in Greece for class A vessels from 31 December 2016 and for class B vessels, it applies from 31 December 2018.

On domestic journeys, the liability of the carrier is regulated by Greek law. In respect of the carriage of passenger vehicles, the Hague-Visby Rules apply instead of the Greek CPML. If a passenger has suffered injury during the carriage that is attributable to the carrier's negligence, he or she is entitled to receive damages (including damages for loss of income and emotional distress). The passenger is also entitled to recover all directly resulting losses in cases where the accident occurred as a result of a fault in the ship's command or navigation by the vessel's master.

vii Seafarers' rights

Greece has ratified the Maritime Labour Convention 2006 and the Prevention of Accidents Convention, 1970 (No. 134) of the International Labour Organization.

Main Activities Performed:

Maritime transport

- Deep-sea shipping - UNCTAD, 2011 ELSTAT,2010, Ministry of Shipping, Maritime Affairs and the Aegean Experts Knowledge Study on EU seafarers' employment –Final Report11
- Short-sea shipping (incl. Ro-Ro) - EUROSTAT,2010, ELSTAT, 201212

- Passenger ferry services - EUROSTAT,2011, XRTC,2010/2011

Food, nutrition, health and eco-system services

- Fishing for human consumption - ELSTAT, 2011, General Directorate for Fisheries,2013
- Marine aquaculture - JRC, 2012 FAO, 2010 ELSTAT,2010
- Agriculture on saline soils - JRC, 2010 DIS4ME15

Energy and raw materials

- Offshore oil and gas - Institute of Energy for South East Europe, 2012
- Offshore wind - HWEA Wind Energy Statistics, 2012
- Ocean renewable energy - WavePlam, 2013
- Carbon capture and storage - Bellona Foundation, 2010
- Securing fresh water supply (desalination) - University of Patras, 2012

Leisure, working and living

- Coastal tourism - Foundation for Economic & Industrial Research, 2012
- Yachting and marinas - Invest in Greece, 2013 HCS, 2012
- Cruise tourism - European Cruise Council (ECC), 2011

Coastal protection

- Protection against flooding and erosion - Policy Reseach Corporation, Country report, 200916
- Preventing salt water intrusion - Gaaloul et al., 2012
- Protection of habitats - Greek Biotope/Wetland Center, The Goulandris natural History Museum,2013

Maritime monitoring and surveillance

- Prevent and protect against illegal movement of people and goods - Ministry of Shipping, Maritime Affairs & the Aegean
- Environmental monitoring - Poseidon system, 2013 Clean SeaNet, 2013 ITOPF, 2012

Other sectors

- Shipbuilding and ship repair - CESA, 2011 ECOTEC,20069 ELSTAT,2010
- Water projects - INVEST IN GREECE, 2010

Impact Towards National Posture:

Greece remains a global shipping stronghold, while Greek Ship Owners, as leaders in the sector, control roughly 20% of the global fleet in terms of capacity. Greek ship ownership is on the rise, surpassing global growth rates in terms of supply (both in number of ships and in available capacity), effectively positioned for an anticipated market recovery.

Greek Ship-Owners continuously renew and expand their fleet with an age profile well below the world fleet's average.

Despite the recent economic crisis, the Greek shipping industry has held well, exceeding the performance of the overall economy both in terms of output and in terms of employment sustained.

Additionally, the Shipping industry plays a crucial role in the Greek economy in terms of produced economic activity, sustained employment, national GDP creation and public revenues.

The total contribution in terms of job created or sustained by Shipping, including indirect and induced employment, exceeds 160,000 and surpasses 3% of total Greek employment.

Moreover, in terms of social impact, the shipping activities also enhance the communication at national level. Also, an important number of independent social responsibility contributions have been made by Ship-owners through foundations that carry their names, individually, or even anonymously.

Barriers and Challenges:

As the wave of consolidation and globalization continues, Greek shipping faces new challenges and barriers:

Maritime research

- Support via funds the State Universities, as are the only to show a systematic and continuous support for Maritime Research.
- Underdeveloped private institutes or Bodies of Maritime/ Marine education or research.

Development & Innovation

- Lack of coordinated promotional campaign with export orientation.
- The Greek ship repair industry is in an unprecedented crisis due to various internal and external reasons. Greek owners seem distracted by this uncompetitive and somewhat problematic sector that cannot be supported anymore by State funding.

Maritime clusters

- Improve cooperation between SME.
- Identification of an institutional body for organizing the clustering of sector actors.
- Encourage funding for promoting and facilitating the clustering of the actors.

Education, training & skills

- Encourage funding for State Universities.
- Limited private initiatives that do not enjoy the support of the Greek State.

Integrated local development

- Political instability and the fragile economic environment of the country has led many investors to flee the country.
- Raise local awareness on impacts and alternative activities developed in each area.
- Boost coordination of actions between policy planning authorities and the stakeholders of the market.

Identified needs and gaps:

Below are presented main areas, where concerted effort could potentially improve the competitiveness of Greece as a whole, as a maritime centre.

- **Education**: Although Greece is known for its maritime education, there are certain issues that need to be reviewed with a view to the new age of the shipping industry. Marine and

maritime educational institutions need to be strengthened while young Greeks need to be encouraged to consider the option of a career in the shipping industry.

- **Ship management**: Ship ownership and ship management remained in Greece, despite economic crisis and capital controls. But increasingly, Greek ship owners need to face the strategic challenge of the transition to the new generation.
- The provision of supplies and equipment to ocean going vessels is considered an export activity and is exempt from taxes.
- **Regulation**: A more business-friendly regulatory environment which will facilitate establishing and operating a shipping-related business in Greece is urgently needed.
- **Ship Repair Industry**: As demand exceeds supply and Greece is in an advantageous geographical position, the opportunity of becoming a ship repair destination should not be left unexploited.
- **Infrastructures** need to be upgraded in order to improve the ports' accessibility and connectivity.

A closer coordination of private sector initiatives aimed at establishing a competitive Greek shipping cluster will also help in promoting its image globally. There is need to enhance and take better advantage of the Greek Maritime Cluster.

5.2.5 Italy

Identified initiatives

The interest toward cybersecurity in the maritime sector started to gain interest in recent years in Italy, mainly after the ransomware campaigns of 2017. Some public events on the subject, aimed at maritime professionals and enterprises have been organised by different bodies during the last years.

A number of Italian universities participate in different project and initiatives on maritime cyber security; as an example, it is worth mentioning Università degli Studi di Genova that, in 2017, conducted studies on cyber risk management especially applied to port security.

The following documents from Guardia Costiera (Italian Coast Guard) address the cyber risk and its evaluation in the maritime sector:

- Circolare Security n° 35 - Cyber Risk Management[232]
- Circolare Titolo Security nr. 40 - Maritime cyber risk management[233]

Regulatory Framework

- The Decreto Legislativo 18 maggio 2018 n. 65, receiving at national level the EU Directive 2016/1148, applies to individuated OSE (Operatori Servizi Essenziali, in Italian) of the maritime sector. OSE list is not a public document, but due to the great numbers of commercial ports and maritime operators Italy, it is almost sure that at least the more prominent among those are included in that list.
- The Decreto Legislativo 10 agosto 2018, n. 101, even if not specific to the maritime sector, it receives at national level the EU Regulation 016/679 (GDPR) about Data Privacy.
- The DECRETO LEGISLATIVO 10 agosto 2018, n. 101[234]
- The Annual Report 2018 on security of navigation SESTO REPARTO – SICUREZZA DELLA NAVIGAZIONE[235].
- MSC 98 MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems (entering in force January 1st 2021)

Main Activities Performed

Aside the institutional initiatives, a number of local ones are developed by diverse actors of the maritime ecosystem.

Those activities are mainly aimed at forming a basic to middle level cybersecurity awareness, both at a management level, in order to stimulate the application of the necessary measures to comply to the regulation on time for the 2021 deadline; and at a more operative level, even if

[232] http://www.guardiacostiera.gov.it/normativa-e-documentazione/Documents/Circolare n_35.zip
[233] http://www.guardiacostiera.gov.it/normativa-e-documentazione/Documents/040_Circolare_Security nr. 40.zip
[234] https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg
[235] https://www.guardiacostiera.gov.it/stampa/Documents/annual-report-2018/AnnualReport2018.pdf

in this case those initiatives are not yet officially fully integrated as part of the curriculum studiorum of the maritime personnel.

Impact Towards National Posture

The project will have a sustained and positive impact on the national maritime sector posture on cybersecurity awareness and cyber threats preparedness. This impact will be achieved by largely improving the ability of the different operators of the maritime sector to integrate cybersecurity best practices and procedures in their already set security and safety frameworks and to better cope with cybersecurity incidents handling.

The proposed work will surely have an effective impact on the national posture in terms of compliance to the NIS directive, being also addressed to maritime OSE operators.

Another beneficial impact of the proposed project will consist in the effective enhancement of the practical knowledge of cybersecurity topics across all levels of the maritime workforce. A holistic playground, integrated with already existing scenarios simulations to experiment the complexity of cases with added cybersecurity, will be available for a comprehensive training of the personnel. This will improve their whole preparedness and qualification and will foster greatly their ability to successfully confront with real situations and to cope with the dynamic evolution of the cyber threats.

Finally, the whole national supply chain security posture will be impacted by the project outcomes, due to the improvements induced in one of its pillars.

Barriers and Challenges

Three factors are identified as drivers that could be the turning points on the Italian Maritime Economy: (i) the infrastructural integration (a.k.a., intermodality); (ii) foreign investment attraction for which the establishment of Free Zones can be a decisive factor; And (iii) a renewed need for a change in conceiving logistics; not just as a mere sector to revive but as a development factor for competitiveness that must be high on Italy's agenda [IME15].

Identified needs and gaps

The main identified need which has to be satisfied for the whole maritime sector is rapidly improving the awareness, preparedness and ability to react to cybersecurity threats and incidents in a sustainable way by including those aspects in the already existing safety and security framework. In order to achieve this goal, it has to be considered the contextual strong need of enabling operators along the whole hierarchy to access up to date information and tools in order to enable them in applying the opportune measures to successfully confront the cyber threats and to reduce the related risks.

The gaps reside mainly in the very nature of the maritime industry: multicultural work forces, workplaces diffused around the world, a fast pace work environment with strong pressures for

economic viability of the chosen solutions. An extra effort is required at all levels in improving the awareness and knowledge of cyber security fundamentals so to address those gaps in an efficient and fruitful way. The prompt availability of holistic solutions that combine technical and economic feasibility with the easiest possible implementation while smoothly integrating in the already existing safety and security frameworks is a way to reduce those gaps and satisfy the identified needs.

5.2.6 Spain

Identified initiatives

Spain has the National Centre for Infrastructure Protection and Cybersecurity, namely CNPIC[236] (Centro Nacional de Protección de Infraestructuras y Ciberseguridad).

Regarding cybersecurity issues, vessels are covered by IMO[237] regulation, Puertos del Estado[238] is a public entity under the Ministry of Transport, Mobility and Urban Agenda of Spain, with global responsibilities over the entire state-owned port system

Regulatory Framework

- Law 14/2014 Maritime Navigation,[239] which updates the maritime regulation, dealing with the existing gaps and incoherencies between the IMO Conventions signed by Spain.
- Royal Decree 145/1989 National Regulation of Admission, Handling and Storage of Dangerous Goods in Ports[240]
- National Maritime Security Strategy[241], which adapts the national strategy to the requirements of the maritime sector
- Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security
- Royal Decree 1617/2007, de 07 of December (BOE 20), measures to improve the protection of ports and maritime transport, (in application of Directive 2005/65 /EC)

Main Activities Performed

Spain is aligned with the international initiatives in the field of maritime safety, including the main legal instruments and the bases for the exercise of State authority at sea. The processes of coordination and cooperation within international and regional organizations are noted, with particular attention to the action of the North Atlantic Treaty organization (NATO242) and the European Union.

These regional organizations, of which Spain is a member, have developed strategies based on the close interdependence between maritime security and other broader interests; this is the case of the North Atlantic Treaty Organization, with its 2011 Maritime Strategy, and the

[236] http://www.cnpic.es/
[237] http://www.imo.org/es/Paginas/Default.aspx
[238] http://www.puertos.es/es-es
[239] http://www.cnpic.es/Legislacion_Aplicable/Sector_Transporte/docs/LEY_14_2014_NAVEGACION_MARITIMA.pdf
[240] http://www.cnpic.es/Legislacion_Aplicable/Sector_Transporte/docs/A04261-04287.pdf
[241] http://www.cnpic.es/Biblioteca/Legislacion/Generico/20131205_Estrategia_de_Seguridad_Maritima_Nacional.pdf
[242] https://www.nato.int/

European Union, within whose framework work has been underway since 2010 on a European Maritime Security Strategy.

As in other sectors, the use of ICTs in the maritime domain increases the likelihood of cyber-attacks against elements that are essential for the development of maritime activities.

For this reason, CNPIC has been taken the necessary measures to protect surveillance and control systems, critical maritime infrastructure and navigation and communication systems.

In the field of Response to Information Security Incidents in Critical Infrastructures is set up the Security Incident Response Team specialized in the analysis and management of technological security problems and incidents related to critical infrastructures at national level in the private sector.

In the event that a Critical Infrastructure suffers a cyber-security incident, the operator responsible for it may benefit from the services of the corresponding response team.

Impact Towards National Posture

- Adoption of a comprehensive approach to enhance the coordinated and cooperative action of the various administrations in solving problems affecting maritime safety
- Adoption of effective and efficient measures in an optimal use of available resources
- Fostering international cooperation
- Fostering collaboration with the private sector

Barriers and Challenges

Taking into account that ports are considered as critical infrastructures, cybersecurity controls in this area is already high in Spain. The main challenge it is therefore to keep both security and safety to high standards in all ports and shipping operations.

Identified needs and gaps

The essential nature of ICTs in the maritime domain requires that concrete actions be established within the framework of cybersecurity in order to contribute to the improvement of national maritime security standards.

There is a need to promote a comprehensive approach to cybersecurity based on the assessment of maritime-specific cyber risks and threats, as well as the identification of all critical assets in the sector.

In order to limit the negative effects of a cyber-attack, actions will be supported aimed at increasing capacities for prevention, defence, detection, exploitation, analysis, recovery and coordinated response to cyber-threats in the maritime space.

Cybersecurity aspects will be added to the Telecommunication Networks and Maritime Information Systems, as well as in the development and application of technologies to strengthen security structures, surveillance capacity, and the ability to prevention and response systems.

The exchange of information, cooperation and public-private partnership also in the international environment, as well as the development of standards and best practices in cybersecurity in the maritime domain are also priority actions.

There is also a need to build up a framework of expertise on the subject aimed at professionals in the maritime field, as well as actions to raise awareness and awareness in this specific field.

Additional Information:

The National Security System has developed an organization structure under the direction of the President of the government, composed of the following entities:

- the National Security Council;
- the Specialized Committee on Maritime Security;
- the Specialized Committee on the Situation, which is unique for the whole Security System National.

5.2.7 Sweden

Identified initiatives

The maritime sector is increasingly using automation and integrated digitized systems, which opens up the possibility of data breaches. With the development of technology, information technologies (IT) are intertwined with operational technologies (OT), often via the Internet, to integrate entire shipping organizations. The development is both necessary and welcome at the same time, increasing the risks of unauthorized access to data, harmful attacks on vessels 'operating systems, shipping companies' business systems and networks. In order to minimize risks with this, management for shipping companies should develop risk management that also aims to include cyber security.

Cyber security is discussed internationally, including IMO already adopted resolution MSC.428 (98) regarding Maritime Cyber Risk Management in Safety Management System (SMS) as early as 2017. The resolution refers to an approved security organization system (SMS) that is capable of handling risk management even for cyber security in accordance with the existing requirements that exist within the ISM code. The work of integrating cyber security as part of SMS must be completed by the first annual verification of the shipping company's document on approved security organization occurring after January 1, 2021.

The Swedish Transport Agency[243,244] recommends shipping companies to consider digital connections to vessels from, for example, system suppliers of propulsion machines and other operating systems with which the company collaborates, within the framework of risk management for cyber security. Particular focus should be placed on the fact that the security organization system deals with the commander's knowledge of how and when system suppliers affect vital systems on board.

Regulatory Framework

Cyber security is discussed internationally, including IMO already adopted resolution MSC.428 (98) regarding Maritime Cyber Risk Management in Safety Management System (SMS) as early as 2017. The resolution refers to an approved security organization system (SMS) that is capable of handling risk management even for cyber security in accordance with the existing requirements that exist within the ISM code.

IMO has drawn up guidelines published in circular MSC-FAL.1 / Circ.3. The circular contains guidelines for risk management of maritime cyber risk management. The purpose of these

[243] https://transportstyrelsen.se/sv/sjofart/Sjotrafik-och-hamnar/Sjofarts-Hamnskydd/
[244] https://transportstyrelsen.se/sv/sjofart/Fartyg/sjosakerhetsarbete/aktuell-information/

guidelines is to create a better understanding and thereby provide better protection against cyberattacks.

Business organizations have also prepared their own guide “Guidelines on Cyber Security Onboard Ships ” based on IMO resolution MSC.428 (98) and circular MSC-FAL.1 / Circ.3.

Industry guidance also relies on the US National Institute of Standards and Technology (NIST[245]) framework that provides guidance for both internal and external threats when dealing with cyber security. The guidance is not intended to be a basic document for external auditing of the shipping company's ability to handle cyber risks but should be seen as a guiding document directed to shipping companies for how the organization should work on strengthening the organization's cyber security.

IACS (International Association of Classification Societies[246]) has also developed recommendations on cyber security through IACS Rec No 159 (Network security of onboard computer based systems) that can also be used as a basis for working with these issues.

The Swedish Transport Agency recommends shipping companies to consider digital connections to vessels from, for example, system suppliers of propulsion machines and other operating systems with which the company collaborates, within the framework of risk management for cyber security. Particular focus should be placed on the fact that the security organization system deals with the commander's knowledge of how and when system suppliers affect vital systems on board.

Moreover, On December 13, 2002, at a diplomatic conference in London, new rules on maritime security were decided. The reason for this is the events of September 11, 2001 in New York and Washington.

The new rules came into force on July 1, 2004 and are an addition to Chapter V and Chapter XI-1 and a new Chapter XI-2 to the SOLAS Convention. In addition to the rules in SOLAS, a new code, the so-called ISPS code, joined.

Within the EU, the new rules have been put into effect by Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on improved maritime security on ships and in port facilities. Furthermore, the Swedish Parliament has passed a Law (2004: 487) on maritime security and the Government on a Regulation (2004: 283) on maritime security. Finally, the Swedish Maritime Administration has issued a regulation on maritime safety, SJÖFS 2004: 13.

The legislation concerns cargo vessels, including high-speed vessels, with a gross tonnage of 500 or more, passenger ships, including high-speed passenger ships, mobile oil platforms at sea, and port facilities serving vessels operating in international traffic and passenger land between. Since 1 July 2008 tonnage has been applied in accordance with the 1969 measurement rules for vessels in international traffic.

[245] https://www.nist.gov/
[246] http://www.iacs.org.uk/

The vessels, after approval of security plans and on-board control, receive an international maritime safety certificate issued by the Swedish Transport Agency. In the same way, the approved and controlled port facilities receive a declaration of conformity issued by the Swedish Transport Agency.

In addition to the above, the EU has also adopted a directive. Directive 2005/65 / EC of the European Parliament and of the Council on increased port security. The directive has been introduced into Swedish law through a Law (2006: 1209) on port security, a Regulation (2006: 1213) on port security and the Swedish Maritime Administration's regulations on port security (SJÖFS 2007: 1).

A port is defined as a specified land and water area that consists of facilities and equipment that facilitate commercial sea transport. The Swedish Transport Agency approves the port security plans and proof of completed, approved control is noted or appended to the decision.

Main Activities Performed

The Swedish Transport Agency is the supervisory authority for individual operators (companies) who conduct safety-sensitive activities in:

- Civil aviation air navigation service;
- Military aviation traffic management service; and
- Activities that are important in aviation security, maritime security or port security.

The Swedish Transport Agency is also responsible for deciding on placement in safety classes 2 and 3 and on register checks regarding employment or other participation in the activities mentioned above and conducted by private or state-owned companies.

For individual operators within the Swedish Transport Agency's supervisory area, the Swedish Transport Agency also issues regulations on security protection, which complements the regulations of the Security Police. The Swedish Transport Agency also has the task, within its area of supervision, to provide guidance on safety protection.

Impact Towards National Posture

- A holistic approach to promote coordination between different administrations and organizations to enhance maritime safety and security.
- Promote optimal and efficient use resources.
- Promote international, regional, and local, cooperation.

Barriers and Challenges

The main challenges facing the maritime domain are:

- Detection of cybersecurity malicious events in real time;
- Mitigation of complex cyber-physical threats.

Identified needs and gaps

There is not any compulsory framework of cybersecurity in order to contribute to the improvement of national maritime security standards. It is crucial that by a holistic approach and assessment identify maritime-specific cyber risks and threats, as well as all critical assets in the cluster. This will minimise the negative impacts of any probable cyber-attack.

Additional Information:

More and detailed information can be found related to the security from the following regulations[247]:

- Security Protection Act (2018: 585);
- Security Protection Regulation (2018: 658);
- The Security Police Regulations (PMFS 2019: 2) on security;
- Armed Forces Regulations (FFS 2019: 9) on signal protection service; and
- The Swedish Transport Agency's regulations (TSFS 2019: 108) on safety protection.

[247] https://www.sakerhetspolisen.se/en/swedish-security-service/protective-security.html

5.2.8 United Kingdom

Identified initiatives

The main initiatives in the maritime domain are:

- Maritime Research & Innovation UK[248]
- Maritime Futures[249]
- Maritime UK Autonomous Systems Regulatory Working Group[250]

Regulatory Framework

Maritime safety is fulfilled by the Maritime and Coastguard Agency (MCA), Marine Accident Investigation Branch (MAIB), the three General Lighthouse Authorities (GLAs) and a small team the Department Of Transport.

The Maritime and Coastguard Agency (MCA) enforces the rules to which vessels in UK territorial waters and under UK registration must adhere. These rules are legislated through the Merchant Shipping Regulations, which apply to all vessels under the UK flag and vessels in UK waters or operating from UK ports.

The IMO is the UN agency that regulates the international shipping industry. It aims to provide a regulatory framework covering safety, environmental concerns, legal matters, technical co-operation, maritime security and the efficiency of shipping.

Main Activities Performed

The main activities of the MCA include:

- Providing round the clock maritime search and rescue around the UK coast, and international search and rescue through HM Coastguard.
- Ensuring the safety of all persons travelling on a vessel in UK territorial waters.
- Ensuring the safety of all seafarers on UK flagged vessels.
- Ensuring that all equipment on UK vessels is fit for purpose and conforms to maritime regulations and standards
- Ensuring that all seafarers on UK vessels have correct documentation
- Ensuring that the environment around the UK coasts and around UK territorial waters is up to standard.
- Ensuring that the hydrographic data on UK charts in accurate.
- Overseeing coastal rescue volunteers, seafarer certification and the port state control inspection regime.

[248] https://www.maritimeuk.org/programmes/innovation/research-innovation/
[249] https://www.maritimeuk.org/programmes/innovation/futures-programme/
[250] https://www.maritimeuk.org/programmes/innovation/maritime-uk-autonomous-systems-regulatory-working-group/

Impact Towards National Posture

The MCA strives to ensure that the UK is a world leader in maritime safety and hydro graphics. To this end, the MCA runs several programmes that aim to promote, assess and audit the safe use of maritime resources.

The Department of Transport is responsible for the implement of the UK's maritime safety action plan, Guide to Good Practice and the Port Marine Safety Code. The Port Marine Safety Code is voluntary guidance that was, and continues to be, developed in partnership with the industry. It is used by all marine facilities in the UK but its quality and effectiveness has also been recognised internationally with a number of countries having adopted it for their own purposes.

The UK is already a hot bed of safety innovation with a large number of small firms producing world-leading and state of the art products. The General Lighthouse Authorities' Research and Development team (GRAD) take forward ground-breaking work with physical and radio marine aids to navigation, support systems and their integration to support the GLA's mission to deliver a reliable, efficient and cost-effective aids to navigation service for the benefit and safety of all mariners.

Barriers and Challenges

Since its high point in around 2009, the UK ship register has declined by some 17 percent measured in gross tonnage. The size of the UK's interest in shipping has decreased over the last 5 years, with the number of UK registered ships falling. The main cause of the decrease in the size of the UK fleet has been the net impact of ships transferring their registration to other countries, with fewer ships transferring their registration from elsewhere to the UK.

The security of the maritime industry is an emerging but increasingly important challenge. The growing digitization of the naval systems increases the attack surface of maritime information systems. Maritime information systems, whether on board of ships or in ports, are numerous, built with standard components available on the market and in many cases designed without accounting for the cyber risk, which is ever-growing.

Identified needs and gaps

Ships are becoming increasingly complex and dependent on the extensive use of digital and communications technologies throughout their operational life. Poor security could lead to significant loss of customer and/or industry confidence, reputational damage, potentially severe financial losses or penalties, and litigation affecting the companies involved. This vitally important aspect of maritime is still in its infancy with many gaps that are yet to be filled.

5.2.9 Maritime Ecosystem Main Findings

Table 13 presents a summary of the main cybersecurity aspects found in the eight European countries that participated in the study.

Table 13. Maritime Ecosystem in Europe Main Findings

Finland	France	Germany	Greece
			
- Several national initiatives in the maritime sector - Goal of operating autonomous maritime ecosystem by 2025 - Large number of cargo ports which are all different in ownership, size, location, clients and physical/ICT system infrastructure - No cybersecurity standards within maritime domain - Lack of cybersecurity preparedness and awareness.	- Thrust building between public and private entities has been initiated in 2019around several maritime initiatives - global cybersecurity strategy for the maritime domain including ships and harbours. - only terrestrial, maritime and port infrastructures seem concerned in terms of digital vulnerability of ships - SME's contribution to the maritime sector is high, even though limited security capacities.	- Several existing initiatives in the maritime domain - Regulatory framework is vast for the maritime sector on global, regional and national levels, however very little consideration is given to cyber security elements - Modern high-tech shipbuilding and shipbuilding supply industries, its globally leading shipping companies - Lack of skilled labor.	- Strong regulatory framework that covers safety; port state controls; registration and classification; environment; collision, salvage and wrecks; passenger's rights; and seafarer's rights. - Infrastructures need to be upgraded in order to improve the ports' accessibility and connectivity. - Lack of coordinated promotional campaign with export orientation - Need closer coordination of private sector initiatives aimed at establishing a competitive Greek shipping cluster.

Italy	Spain	Sweden	United Kingdom
			
- Connection of maritime cybersecurity only started in recert years - Need of improving awareness, preparedness and ability to react to cybersecurity threats and incidents in a sustainable way by including those aspects in the already existing safety and security framework. - Need of enabling operators along the whole hierarchy to access up to date information and tools to successfully confront the cyber threats and to reduce the related risks.	- Mature regulatory framework in port and maritime transport - Need to promote a comprehensive approach to cybersecurity based on the assessment of maritime-specific cyber risks threats, and critical assets in the sector - Need to build up a framework of expertise on the subject aimed at professionals in the maritime field, as well as actions to raise awareness and awareness in this specific field.	- Regulatory framework is vast about maritime cybersecurity management - Currently working on a holistic approach to promote coordination between different administrations and organizations to enhance maritime safety and security - No compulsory framework of cybersecurity to contribute to the improvement of national maritime security standards.	- Several initiatives and programmes currently running to promote, assess and audit the safe use of maritime resources. - The size of the UK's interest in shipping has decreased over the last 5 years, with the number of UK registered ships falling. - Security aspects of maritime are still in their infancy with many gaps that are yet to be filled.

6. Maritime Cybersecurity in Europe

6.1 Main Authorities

At a broader level, we can place the European Commission (EC) as one of the main authorities in the cybersecurity and maritime related aspects in Europe (See Figure 6). Maritime security[251] is a key objective of the EC as it belongs to one of the five transport modes (i.e., air, road, rail, maritime, and inland waterways). The EU's maritime security policy explicitly states that its overall objective is to protect the citizens and their economies from the consequences of unlawful intentional acts against shipping and port operations.

The EU has been given the obligation by the European Parliament and the Council to monitor the application by Member States of the Maritime Security legislation and to verify the effectiveness of national maritime security measures, procedures and structures. In order to fulfil this task, the Commission adopted a Regulation on procedures for conducting Commission inspections in the field of maritime security.

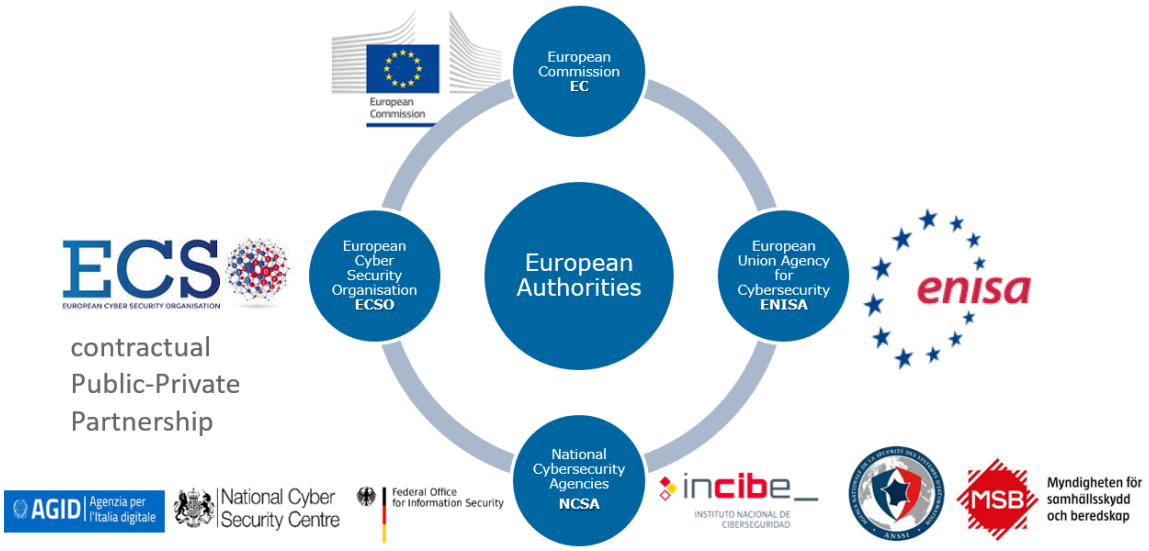


Figure 6. Cybersecurity and Maritime Authorities

Several organizations have been created to apply and control the regulations established by the EC about cybersecurity related aspects in specific industrial sectors (including the maritime domain). Examples of these organizations are the European Cybersecurity Organization (ECSO[252]), whose main goal is to develop a competitive European cybersecurity ecosystem, to support the protection of the European Digital Single Market with trusted cybersecurity solutions, and to contribute to the advancement of the European digital autonomy. ECSO is the private counterpart to the European Commission in implementing the contractual Public-Private Partnership (cPPP) on cybersecurity, for which it has developed a National Public Authority Committee (NAPAC) and six working groups to promote diverse aspects such as standardization, market deployment, training, cybersecurity technologies, among others.

[251] Maritime Security https://ec.europa.eu/transport/modes/maritime/security_en
[252] https://ecs-org.eu/

Similarly, the European Union Agency for Cybersecurity (ENISA[253]) has been created to contribute to European cybersecurity policy, supporting Member States and European Union stakeholders as a response to large-scale cyber incidents that take place across borders in cases where two or more EU Member States have been affected.

National Cybersecurity Agencies (NCSA) have been created in all EU countries, aiming to defining National Cybersecurity Strategies that will be in line with ENISA and other organization authorities. As of June 2020, all EU member states possess a National Cybersecurity strategy as presented in the previous sector by the eight selected European countries.

6.2 European Market

According to a recent research study regarding the cybersecurity market in Europe [GLO19], three clusters have been identified among the targeted countries based on their size of the market, level of competition, maturity, policy framework and market accessibility (Figure 7):

(i) Cluster 1 (UK, Germany, France, the Netherlands), Large and competitive markets supported by strong regulation from national authorities, and strong capacities of the public authorities;

(ii) Cluster 2 (Belgium), Smaller and less mature market, presence of international organizations and large firms in the private sector, market attraction from neighbouring European countries; and

(iii) Cluster 3 (Spain, Italy, and Poland), Relatively small size of Cybersecurity markets, significant structural economic challenges and/or lack of public investment.

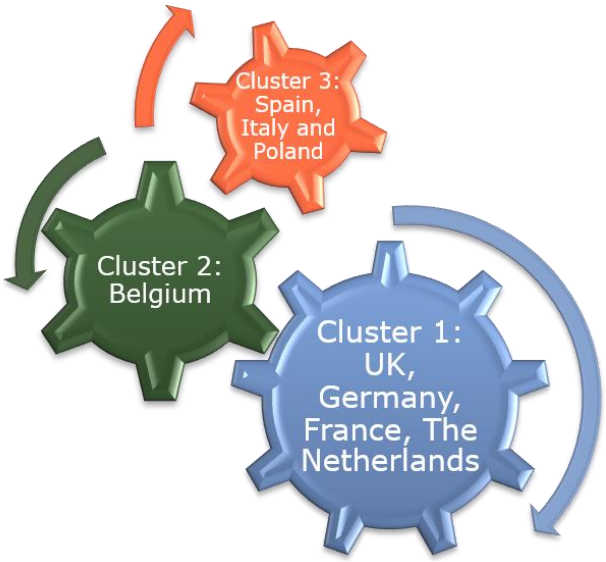


Figure 7. Cybersecurity and Maritime Authorities

In general terms, the conducted research identified that although there are significant differences among the markets of the target countries, there are continued levels of growth across each market. In addition, most EU institutions and Member States are strengthening

[253] https://www.enisa.europa.eu/

their regulatory framework to improve cybersecurity by ensuring safety and resilience of the economy and society; and although some countries perform well in several features regarding market attractiveness and accessibility, there are still neutral and negative aspects to be considered before doing business in Europe. Table 14 summarizes the main aspects of each of the eight countries selected for this study.

Table 14. Cybersecurity Market Conditions in Europe

United Kingdom	Germany	France	The Netherlands
			
- Leading Cybersecurity market in the world. - Open and legally structured to welcome foreign companies, yet highly competitive. - Dominant role of public security actors	- Very mature market with a tendency to grow and expand - Opportunities remain for those offering niche, high-quality technology in the industrial sector - Dominant role of public security actors	- One of the most mature and regulated markets in Europe - Plenty support of Government - Growth is still expected, although polarized by few large players and small/micro firms	- Highly digitized economy and one of Europe's leading markets - Strong international player presence, which both facilitates the entry of foreign actors and raises the risk of future saturation
Belgium	**Spain**	**Italy**	**Poland**
			
- Government support and a €15bn investment plan - Opportunities for niche technologies and services - Mature market with regional disparities	- Rapidly expanding market driven by a handful of large companies - Opportunities for niche technologies and services - Public and private actors' interest and potential to market entry into Latin America	- Smaller and less mature market - Support for the digitization of public administration sector and industry - Potential commercial opportunities for services and product providers	- Growing IT sector with Government support - Market far from saturated with cybersecurity hub aspirations - Importance of EU funds in investment efforts

As a result of the previously presented study, researchers highlight that cybersecurity has become a priority for governments, companies and citizens in all European countries. With the digital transformation in all sectors of society (including the maritime sector), cybersecurity takes a crucial part with growing needs for smart and user-friendly solutions designed to secure digital systems at large.

6.3 Global Cybersecurity Index

Considering the fact that not all countries use the same type of technologies and are not equally developed, it is logical to expect a variety on their cybersecurity maturity level. The International Telecommunication Union (ITU[254]) has developed a Global Cybersecurity Index (GCI) for which a report is released every year to assess the cybersecurity commitment and situation worldwide. According to the latest report [GCI18], 25 indicators have been evaluated referring to the following pillars of the Global Cybersecurity Agenda:

1. **Legal**: Measures based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.

2. **Technical**: Measures based on the existence of technical institutions and framework dealing with cybersecurity.

3. **Organizational**: Measures based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.

4. **Capacity building**: Measures based on the existence of research and development, education and training programmes, certified professionals and public sector agencies fostering capacity building.

5. **Cooperation**: Measures based on the existence of partnerships, cooperative frameworks and information sharing networks.

Each of the pillars are assessed in a scale 0-200, the addition of the five pillars makes the final GCI score to range from 0 - 1,000. A total of 194 countries participate in the study, grouped in six main regions (i.e., Europe, from which European countries, Commonwealth of Independent States – CIS, Asia-Pacific, Arab state, Americas, and Africa), from which Europe provides the highest scores in most of the indicators. The GCI is useful to identify areas for improvement, illustrate the practices of others so that countries can implement them, and thus helping to harmonize practices and foster a global culture. Table 15 provides information of the GCI of the top 10 countries in the study.

[254] https://www.itu.int/en/Pages/default.aspx

Table 15. Top 10 Global Cybersecurity Index

Rank	Country	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
1	UK	0.931	0.200	0.191	0.200	0.189	0.151
2	USA	0.926	0.200	0.184	0.200	0.191	0.151
3	France	0.918	0.200	0.193	0.200	0.186	0.139
4	Lithuania	0.908	0.200	0.168	0.200	0.185	0.155
5	Estonia	0.905	0.200	0.195	0.186	0.170	0.153
6	Singapore	0.898	0.200	0.186	0.192	0.195	0.125
7	Spain	0.896	0.200	0.180	0.200	0.168	0.148
8	Malaysia	0.893	0.179	0.196	0.200	0.198	0.120
9	Norway	0.892	0.191	0.196	0.177	0.185	0.143
10	Canada	0.892	0.195	0.189	0.200	0.172	0.137

From Table 13, we can identify that six countries from the Europe region are included in the top 10 GCI scores, with the United Kingdom as the leader of the list, having a score of 0.931 (accounting the maximum score for the Legal and Organizational pillars). Taking a more global perspective, 30 countries in the European region have been assessed with a high GCI (0.670 - 1.000); 12 countries have been assessed with a medium GCI (0.340 - 0.669); and only 4 countries have been assessed with a low GCI (0.000 – 0.339).

The main outcome for this study is that none of the countries attaint the maximum score in all the pillars, being the Cooperation pillar the one with the lowest individual scores among the participant countries. Some of the top-10 countries reached the maximum score in the Legal and Organizational pillars, showing strong foundations in legal and regulations dealing with cybersecurity as well as in the definition and implementation of national cybersecurity strategies.

6.4 Challenges vs Initiatives in the EU

ENISA has realised a report on cybersecurity challenges in the maritime sector in 2011 [ENI11], and very recently, as a report on port cybersecurity in 2019 [ENI19]. In the 2011 report, the level of maritime cybersecurity awareness is assessed as low to non-existent. Adapting maritime cybersecurity to the high ICT complexity is one of the major challenges to face. Moreover, as maritime regulations and policies consider mainly physical aspects of security and safety, policies including both cyber and physical domains are an open issue. In the 2019 report, the lack of digital culture in the port ecosystem, the lack of awareness and training

regarding cybersecurity, the lack of time and budget allocated to cybersecurity, and the lack of human resources and qualified people in the maritime cybersecurity domain, are among the main challenges currently faced by ports to implement cybersecurity measures.

The following challenges appear to be common in most European countries that participated in the Cybersecurity and Maritime Ecosystem study from Section 5.

Challenges

- Evolvement of cyber espionage and cybercrime
- Knowledge leak and loss of control in key areas
- International competition in the sector
- Poor bilateral and multilateral collaboration
- Non-existing legal basis for collaboration
- Lack of qualified personnel
- Lack of funding
- Lack of trust between organizations
- Lack of legal settlement to improve sharing mechanisms
- Need for common standards, semantics and processes implemented in interoperable solutions
- No proper coordination of activities in the sector
- Lack cybersecurity awareness
- New vulnerabilities and complex cyber-attacks with potential disastrous consequences
- Poor cyber hygiene and compliance

From the previous list, lack of cybersecurity awareness, lack of qualified personnel and poor bilateral/multilateral collaboration appear to be the top challenges to be faced by any organization from the maritime industry. Several initiatives have been defined in order to cope the aforementioned challenges. The following list summarizes such initiatives.

Initiatives

Various initiatives have been developed to promote cybersecurity in the maritime sector. The following initiatives appear to be common in most European countries that participated in the Cybersecurity and Maritime Ecosystem study from Section 5.

- National Cybersecurity Centres and Agencies
- National Cybersecurity Strategies
- National Information Sharing and Analysis Centres
- IT security in Business (SMEs)
- IT for Business Protection (government and industry cooperation)
- National plans to protect Critical Infrastructures
- Training programmes and activities
- EU funded projects
- National funded projects
- Public-Private Partnerships (PPP)

Several EU projects are actively working in the research and development of cybersecurity solutions in the maritime domain. Table 16 compiles initiatives in which at least one Cyber-

MAR partner is also involved. Table 17 refers to past EU projects related to cybersecurity and maritime areas.

Table 16. Active Cybersecurity and Maritime EU Projects

Project	Description	Dates	Key Partner
FORESIGHT[255]	Advanced cyber-security simulation platform for preparedness training in Aviation, Naval and Power-grid environments	01/10/2019 - 30/09/2022	University of Plymouth
PALAEMON[256]	A holistic passenger ship evacuation and rescue ecosystem	01/06/2019 - 31/05/2022	ATOS Spain
THREAT-ARREST[257]	Cyber Security Threats and Threat Actors Training - Assurance Driven Multi-Layer, end-to-end Simulation and Training	01/09/2018 – 31/08/2021	ATOS Spain
HiSEA[258]	High Resolution Copernicus-Based Information Services at Sea for Ports and Aquaculture	01/01/2019 - 30/06/2021	Fundación Valencia Port
CyberTrust[259]	Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things	01/05/2018 – 30/04/2021	University of Plymouth
CYBERWISER[260]	Civil Cyber Range Platform for a novel approach to cybersecurity threats simulation and professional training	01/09/2018 – 28/02/2021	ATOS Spain
HOLISHIP[261]	HOLIstic optimisation of SHIP design and operation for life cycle	01/09/2016 - 31/08/2020	Naval Group
SAURON[262]	Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports	01/05/2017 - 30/04/2020	Fundación Valencia Port

Source: https://ec.europa.eu/easme/en/european-maritime-and-fisheries-fund-0

Table 17. Past Cybersecurity and Maritime EU Projects

Project	Description	Dates
CY CISE[263]	aims to develop the Cypriot information sharing environment towards an integrated national maritime surveillance awareness, complying with the overall European CISE vision. It builds on the knowhow developed within the Hellenic CISE project	01/01/2017 - 31/10/2018
InBulMarS[264]	Integrated Bulgarian Maritime Surveillance, aims to conducting preparatory studies in order to identify the needs and requirements for the improvement of cross-sectoral information exchange for maritime surveillance within and	01/01/2017 - 31/12/2018

[255] https://cordis.europa.eu/project/id/833673
[256] https://palaemonproject.eu/
[257] https://www.threat-arrest.eu/
[258] https://hiseaproject.com/
[259] https://cyber-trust.eu/
[260] https://cyberwiser.eu/
[261] http://www.holiship.eu/
[262] https://sauronproject.eu/
[263] https://ec.europa.eu/easme/en/cypriot-information-sharing-environment-towards-integrated-national-maritime-surveillance-awareness
[264] https://ec.europa.eu/easme/en/integrated-bulgarian-maritime-surveillance

	between EU Member States.	
SHAREMARE[265]	Spanish mAritime Information Sharing system SAIS, aims to develop and then deploy in their current IT framework an information sharing platform.	01/01/2017 - 31/12/2018
MAiDEN[266]	MAritime Information Data Exchange Network, aims to developing an enhanced ICT system to be used at the Maritime Rescue and Coordination Centre (MRCC) and the Maritime Security Centre (MIK).	01/03/2018-29/02/2020
ASSESS[267]	Advanced Skills in Safety, Environment and Security at Sea, is an education and training project focused on professional profiles specialized on safety and security issues related to ships and off-shore plants with three main concerns: safety and security for ships and plants, for people (human life at sea) and for the environment.	01/02/2017-31/01/2019

Source: https://ec.europa.eu/easme/en/EMFF-projects

6.5 Maritime Cybersecurity GAPS in the EU

Although a lot of challenges in the maritime cybersecurity sector are tackled by national and EU initiatives, still there are some of them not being addressed fully (e.g., implementing the right policy, appropriate legal and operational frameworks in place, collaboration with various relevant stakeholders' communities, sharing meaningful cybersecurity information, and prioritizing the protection of critical infrastructures, among others), which represents main issues and gaps in the following key areas [BSA15]:

Legal Foundations: Considerable **discrepancies** exist between member States. National cybersecurity strategies **need further improvements** within the EU. A minority of the Member States have reinforced them with relevant legislative and policy instruments. In addition, most EU member States have not yet assessed their national infrastructures based on objective criteria and subject to public comment to pursue a strategy or plan to protect their most important assets. Furthermore, most EU Member States and public bodies appear not to follow best practices and seem to remain reluctant to introduce standardized data exchange schemes.

Education: Educational and **awareness** raising play a crucial role for governments, industries, and consumers, who need to take steps to secure their own systems. Yet some EU members **need to implement** national education strategies in this field.

Operational Capabilities: While all EU Member States have established operational entities, such as Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs), **their mission and experience vary greatly among the EU**.

Private-Public Partnership (PPP): One notable gap is the lack of systematic cooperation with non-governmental entities and public-private partnerships, thus leaves a

[265] https://ec.europa.eu/easme/en/spanish-platform-maritime-data-share
[266] https://ec.europa.eu/easme/en/maritime-information-data-exchange-network
[267] https://ec.europa.eu/easme/en/advanced-skills-safety-environment-and-security-sea

large area untapped for effective, voluntary collaboration between governments and the private sector that owns and operates the majority of commercial critical infrastructure services in Europe. **Cybersecurity PPP is either non-existent, very restricted**, **or still at a very early stage** of development in the majority of the EU Member States.

Sector-specific Plans: While there is a growing interest in establishing sector-specific responses to cybersecurity, **practical implementation is still fairly limited** in the Member States. In addition, considering that cybersecurity protection is a transversal service across all industries, and that recommendations are established to apply at a national and international context, **there is a need of guidelines** tailored to the business needs of particular entities to address unique risks or specific operations in certain sectors, including the maritime domain.

In addition to the aforementioned gaps, it has been noted from key stakeholders that:

(i) cybersecurity activities (even in the largest ports) seemed to be handled by very few personnel combining with external IT operators;
(ii) There is a gap between IT professionals and end-users that makes is difficult to trace any systematic training program;
(iii) The level of cybersecurity preparedness is directly proportional to the size of the organization (i.e., the smaller the organization's size, the lower the level of cybersecurity preparedness), and
(iv) There is a strong demand of cross-knowledge activities involving awareness and training of maritime cybersecurity related aspects.
(v) Lack of updated reports on cybersecurity challenges, gaps and initiatives in the maritime sector. To the best of our knowledge, the only existing report has been presented by ENISA in 2011 (almost 10 years from the current date).

6.6 Preliminary Recommendations

In order to face the impact due to the COVID-19 situation, the following actions are recommended for shipping organizations [PWC20]:

- Secure as much as possible newly implemented remote working practices, which includes (i) performing continuous risk assessments to existing and new remote access systems, focusing on those used for remotely administering and monitoring IT and OT vessel systems; (ii) reinforce security configuration in remote access solutions to log all authentication events and keep a track on them to detect anomalous activities, and; (iii) ensuring key controls (e.g. web filtering, encryption, antivirus/malware, backups, etc.) are applied to any systems deployed in remote places.
- Ensure the continuity of critical security functions, including (i) continuous monitoring of activities affecting onshore and vessel systems, making user that teams have all necessary resources (e.g., people, processes, technology) to monitor and respond to alerts appropriately; (ii) continuous vulnerability scanning for on-shore and vessel infrastructures to confirm critical vulnerabilities have been patched or mitigated; and (iii) continuous incident response updates to ensure plans work as expected during periods when relevant employees are primarily working remotely.

- Counter opportunistic threats that could take advantage of the COVID-19 situation by providing specific guidance to (i) vessel crews to email communications relating to COVID-19 infections on specific vessels; (ii) finance teams to prevent them from phishing and scamming attacks; (iii) on-shore employees and vessel crews to improve awareness on cyber-attacks using COVID-19 lures. In addition, if possible, implement web filtering technologies and/or attempt to exploit different ways of working.

Additional strategies are proposed to EU Member States to improve their conditions in the maritime cybersecurity area. The following recommendations are based on the different research and reports consulted in the literature and the feedback obtained from Cyber-MAR key stakeholders [ENI11, ENI12, ENI19, BSA15, GCI18].

- Undertake targeted maritime sector awareness raising campaigns and cyber security training of shipping companies, port authorities, national cyber security offices, etc.
- Ensure “security by design” for all critical maritime ICT components.
- Policy makers must consider cybersecurity to physical aspects of security and safety while designing maritime regulations and policies.
- Perform a holistic, risk-based approach; assessment of maritime specific cyber risks, as well as identification of all critical assets within the maritime sector.
- As maritime governance is fragmented between different levels (i.e. international, European, national), the IMO together with the EU Commission and the Member States should align international and EU policies in this sector.
- Better information exchange and statistics on cyber security can help insurers to improve their actuarial models, reduce own risks, and thus offering better contractual insurance conditions for the maritime sector.
- Information exchange platforms should be also considered by Member States to better communications.
- Working towards cybersecurity and cyber resilience with a focus on the protection of critical infrastructure should be an important national priority in all EU member states.
- Join European Commission research projects for network and reputation (e.g. H2020, Horizon Europe programme related to Cybersecurity, European Defence Fund).
- Leverage available networks to gain access to new markets.
- Ensure compatibility and interoperability with target customer’s systems.
- Keep a close eye on European and national legislative developments.
- Privilege the protection of key assets and processes with a cyber insurance company and explore the role of the government as an insurer.
- Enforce security governance of IT and OT environments by describing the roles and responsibilities of each stakeholder (Port Authority, terminal operators, service providers, suppliers, etc.).
- Set up a threat intelligence process to watch continuously for vulnerabilities, identify new risks and threats and deploy actions to mitigate them.
- Ensure identified cyber risks are considered in safety and security plans to align cybersecurity with physical security and safety.
- Address privacy related issues based on applicable local and international regulations, such as the General Data Protection Regulation (GDPR).
- 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.

- 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.
- 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.)
- Set up a security awareness raising program to address the whole port ecosystem, focusing first on the main threats (e.g. social engineering).
- 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.

7. Conclusions

This document presents an ongoing assessment on the regulatory, policy and market watch on the state of play in Europe and in Member States to identify current challenges and initiatives in the maritime cybersecurity domain. This first version of the document aims to catalysing actions and recommendations that support the cybersecurity cPPP, including recommendations to reduce gaps in the area. For this purpose, the document presents three main analysis: (i) Cyber-MAR external factor analysis; (ii) stakeholder analysis, and (iii) Cybersecurity and Maritime ecosystem analysis.

The external factor analysis focused on identifying Political, Economic, Social, Technological, Environmental and Legal (PESTEL) factors affecting directly or indirectly the cybersecurity and maritime domains. The outcome of this analysis indicated that most studied factors fall into the Positive (P) or Very Positive (+P) categories, which in turn reflects an optimal environment for the Cyber-MAR solutions that can be beneficial for the appropriate introduction of the developed assets into the EU market. However, global political conflicts, the EU current economic situation, the cybersecurity maturity in the EU, climate change, and environmental challenges are among the potential negative factors to be considered as threats in Cyber-MAR.

The stakeholder analysis focused on three main stakeholder groups for Cyber-MAR: cybersecurity, shipping, and port. For each of them, internal and external key stakeholders have been identified including consortium partners and external organizations (e.g., clients, providers, competitors, etc.) in the cybersecurity and maritime domain. The analysis uses the interest-power matrix to classify and position key stakeholders into four main categories: key players, context setters, crowd and subjects, for which strategies are proposed to manage and meet the stakeholder needs.

The analysis of the cybersecurity and maritime ecosystem in Europe focused on the national strategies and plans developed by several European countries, and on the identification of aspects related to the regulatory framework, initiatives, challenges and existing gaps in both, the cybersecurity and the maritime industries. Among the challenges in the maritime cybersecurity sector, the lack of cybersecurity awareness, lack of qualified personnel and poor bilateral/multilateral collaboration appear to be common in most studied countries. Several initiatives have been identified in both sectors, with the National Cybersecurity Strategy as one of the major actions taken by all studied countries. The outcome of this analysis is used to propose strategies to reduce existing gaps in the sector and to improve actions and initiatives designed to overcome challenges in the maritime cybersecurity domain. Such strategies will be updated in D8.2 as the final version of this document.

The project has achieved the objectives foreseen in the Description of Action for this deliverable, which represents the initial version of the Cyber-MAR market watch and should be considered as a starting point to define strategies for exploitation and commercialization routes. D8.1 will be continuously updated and complemented with a final version (D8.2) to be released at M36 of the project including detailed actions and recommendations to reduce the supply deficient of cybersecurity training in the maritime domain within the EU.

References

[ABR18] Michael J., Abramowitz. Freedom in the World 2018. Democracy in Crisis. Available at: https://freedomhouse.org/report/freedom-world/2018/democracy-crisis (2018).

[BEE20] Hannah Beech. U.S. Warships Enter Disputed Waters of South China Sea as Tensions With China Escalate. Available at: https://www.nytimes.com/2020/04/21/world/asia/coronavirus-south-china-sea-warships.html (2020)

[BIS19] Marwan Bishara. Arrogance, fanaticism and the prospect of a US-Iranian war. Available at: https://www.aljazeera.com/amp/indepth/opinion/arrogance-fanaticism-prospect-iranian-war-190430085736682.html (2019)

[BJO16] Haugland Bjorn Kjaerand. Towards unmanned shipping. Safety4Sea report available at: https://safety4sea.com/towards-unmanned-shipping/?, (2016).

[BLU18] European Commission. The 2018 Annual Economic Report on EU Blue Economy. Available at: https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/2018-annual-economic-report-on-blue-economy_en.pdf, (2018)

[BOY13] H.A. Boyes. Maritime Cyber Security – Securing the Digital Seaways. In Resilience, Security and Risk in Transport, pp.56-63, (2013).

[BSA15] The Software Alliance. EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace. Available at: http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf, (2015).

[CIS20] CISOMAG, Most U.K. firms suffer basic cybersecurity skills shortage: Research, available at: https://www.cisomag.com/most-u-k-firms-suffer-basic-cybersecurity-skills-shortage-research/, (2020).

[CEP10] Felix Roth and Anna-Elisabeth Thum. The Key Role of Education in the Europe 2020 Strategy. Available at: http://aei.pitt.edu/15058/1/WD338_Roth_and_Thum_on_Education.pdf, (2010).

[CSE20] Cyber Security for Europe. Addressing the shortage of cybersecurity skills in Europe. Available at: https://cybersec4europe.eu/addressing-the-shortage-of-cybersecurity-skills-in-europe/, (2020).

[DEL20] Martin Nyrop, Alexander Nathan, Mads Bocher Lindquist, Jonas Tobias Karlsen. COVID-19 will permanently change e-commerce in Denmark. Deloitte report available at: https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/strategy/e-commerce-covid-19-onepage.pdf, (2020).

[DNV20] DNV-GL. Maritime Cyber Security Awareness E-learning. Available at : https://www.dnvgl.com/maritime/maritime-academy/cyber-security-elearning.html, last visited on May 2020.

[DoA19] Description of Action. Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain, Cyber-MAR, (2019).

[EHT20] Ehtisham Ali. Transformation of E-Commerce Businesses and their Future after COVID-19. Report available at: https://moderndiplomacy.eu/2020/07/07/transformation-of-e-commerce-businesses-and-their-future-after-covid-19/, (2020).

[EMS18] European Commission. Establishing a European Maritime Single Window environment and repealing Directive 2010/65/EU. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018PC0278, (2018).

[EMS20] European Maritime Safety Agency (EMSA). COVID-19 – impact on shipping (Report of July 31st) Available at: http://www.emsa.europa.eu/news-a-press-centre/covid19-impact/item/3967-july-2020-covid-19-impact-on-shipping-report.html, (2020)

[EMT20] European Commission. Maritime Year: EU priorities and actions. Maritime Transport report available at: https://ec.europa.eu/transport/modes/maritime/maritime-transport_en, last visited on May 2020.

[ENI11] ENISA. Analysis of cyber security aspects in the maritime domain. Available at: https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport, (2011).

[ENI12] Neil Robinson. Incentives and barriers of the cyber insurance market in Europe. ENISA report available at: https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe, (2012)

[ENI19] ENISA. Port Cybersecurity – Good practices for cybersecurity in the maritime sector. Available at: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector/, (2019).

[ENI20] ENISA. National Cybersecurity Strategies. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies, last visited on May 2020.

[EPR17] European Commission. Proposal for an ePrivacy Regulation. Available at: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation, (2017).

[ERI18] F., Eriksen-Coats.: What is Mendelow's Matris and How is it useful? Article from the Oxford College of Marketing available at: https://blog.oxfordcollegeofmarketing.com/2018/04/23/what-is-mendelows-matrix-and-how-is-it-useful/, (2018).

[EUC17] European Commission. EU cybersecurity initiatives, working towards a more secure online environment. Available at:

https://ec.europa.eu/information_society/newsroom/image/ document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf, (2017)

[EUC18] European Commission. Maritime Year in Action. Available at: https://ec.europa.eu/transport/sites/transport/files/2018-maritime-year-brochure.pdf, (2018)

[EUC20a] European Commission. Schengen Area, Migration and Home Affairs. Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen_en, (2020)

[EUC20b] European Commission. Free movement – EU nationals, Employment, Social Affairs & Inclusion. Available at: https://ec.europa.eu/social/main.jsp?catId=457&langId=en, last visited on May 2020.

[EUP18] European Parliament. European Maritime Single Window environment, initial appraisal of a European Commission Impact Assessment. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/627160/EPRS_BRI(2018)627160_EN.pdf, (2018)

[EVA17] Michelle Evans. 5 Key tech factors driving the digital consumer in Europe. Euromonitor International Market Research Analysis available at: https://blog.euromonitor.com/key-factors-digital-consumer-europe/, (2017).

[FFU20] Fern Fort University, Diana shipping Inc. PESTEL & Environment Analysis. Available at: http://fernfortuniversity.com/term-papers/pestel/nyse4/2740-diana-shipping-inc-.php, last visited on May 2020.

[FRC16] French Ministry of Environment, Energy and Sea. Cyber Security, Assessment and Protection of Ships. Available on line at: https://www.ecologique-solidaire.gouv.fr/sites/default/files/Guideline%201%20-%20Cyber%20security%20-%20Assessment%20and%20protection%20of%20ship.pdf, (2016)

[FRU17] Markus Fruth, and Frank Teuteberg. Digitization in maritime logistics — What is there and what is missing? Operations, Information & Technology, research article available at: https://www.cogentoa.com/article/10.1080/23311975.2017.1411066, (2017).

[FSEC20] Paul Pratley. State-Sponsored Cyberattacks. F-Secure report available at: https://www.f-secure.com/en/consulting/our-thinking/state-sponsored-cyber-attacks, last visited August 2020.

[GCI18] International Telecommunication Union (ITU). Global Cybersecurity Index (GCI), Annual report available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf, (2018).

[GCT20] Council on Foreign Relations. Global Conflict Tracker. Territorial Disputes in the South China Sea available at: https://www.cfr.org/interactive/global-conflict-tracker/conflict/territorial-disputes-south-china-sea (2020).

[GDP16] EUR-Lex. General Data Protection Regulation, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679, (2016).

[GLO19] Global Ambition. The European cybersecurity Market – Mapping the opportunity and route to market for Irish SMEs. Online available at: https://globalambition.ie/wp-content/uploads/2019/11/The-European-Cybersecurity-Opportunities-for-Irish-SMEs_Key-Takeouts.pdf, (2019).

[GOV18] Government Europa. Innovating for the future of the European maritime sector. Available at: https://www.governmenteuropa.eu/future-of-the-european-maritime-sector/88556/, (2018).

[HAC18]Hackers arise.: Metasploit SCADA Hacking, Post available at: https://www.hackers-arise.com/post/2018/10/22/metasploit-basics-part-16-metasploit-scada-hacking (2018).

[IME15] SRM. Italian Maritime Economy, terminals, logistics and its players: challenges from a pivotal Mediterranean position. Annual Report available at: https://www.srm-maritimeconomy.com/p/italian-maritime-economy-terminals-logistics-and-its-players-challenges-from-a-pivotal-mediterranean-position-annual-report-2015/, (2015).

[INS17] Insurance Europe. Insurers' role in increasing cyber resilience. Available at: https://www.insuranceeurope.eu/insurers-role-increasing-cyber-resilience, (2017).

[INS19] Business Insider. Generation Z, latest characteristics, research, and facts. Available at: https://www.businessinsider.com/generation-z, (2019).

[KAV20] Georgios Kavallieratos, Sokratis Katsikas, Vasileios Gkioulos. Modelling Shipping 4.0: A Reference Architecture for the Cyber-Enabled Ship. In Asian Conference on Intelligent Information and Database Systems, vol. 12034, pp. 202-217, (2020).

[LAG18] Sotiria Lagouvardou. Maritime Cyber Security: concepts, problems and models. Master Thesis, Technical University of Denmark. Resource available online at: https://backend.orbit.dtu.dk/ws/portalfiles/portal/156025857/Lagouvardou_MScThesis_FINAL.pdf (2018).

[LAM17] Maria Lambrou, Masaharu Ota. Shipping 4.0: Technology Stack and Digital Innovation Challenges. In IAME Conference, paper ID 155, available online at: https://www.researchgate.net/publication/320102036_Shipping_40_Technology_Stack_and_Digital_Innovation_Challenges, (2017).

[LEE17] Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, Improving cyber security awareness in maritime transport : A way forward. Journal of the Korean Society of Marine Engineering 41(8), pp. 738-745, (2017)

[LLO20] Lloyd's Register. Training, Maritime Cyber Security Awareness. Available at: https://www.lr.org/en/training/maritime-cyber-security-awareness/, last visited on May 2020.

[MAI20] MAI Custom BPO Solutions, Ruling the Waves: How Politics Can Impact International Shipping. Available at: https://www.mktalt.com/Blogs/ruling-the-waves-how-politics-can-impact-international-shipping.html, last visited on May 2020.

[MAR50] UK Department for Transport. Maritime 2050, navigating the future. Available at: https://www.gov.uk/government/publications/maritime-2050-navigating-the-future, (2019).

[MCS11] European Network and Information Security Agency (ENISA), First EU-report on Maritime Cyber Security. Available at: https://www.enisa.europa.eu/news/enisa-news/first-eu-report-on-maritime-cyber-security (2011)

[MIS18] Baibhav Mishra. Impact of globalization on shipping and maritime industry. Available at: https://seanews.co.uk/features/impact-of-globalisation-on-shipping-and-maritime-industry/ (2018).

[MOR19] Steve Morgan, Cybersecurity talent crunch to create 3.5 million unfilled jobs globally by 2021. Cybercrime Magazine, report available at: https://cybersecurityventures.com/jobs/, (2019).

[MYB20] Beeye Online Tool. Stakeholder analysis, consulted on March 2020, available at: https://www.mybeeye.com/management-tools/stakeholder-analysis

[NAU20] Nautilus International. COVID-19 leaves maritime sector vulnerable to cyber attacks. Available at: https://www.nautilusint.org/en/news-insight/news/covid-19-leaves-maritime-sector-vulnerable-to-cyber-attacks/, (2020).

[NOR18] Norton Rose Fulbright. Impact of Brexit on the transport sector. Available at: https://www.nortonrosefulbright.com/en/knowledge/publications/16d0fc9c/impact-of-brexit-on-the-transport-sector, (2018).

[OIK19] Stergios Oikonomou, Ioannis Filippopoulos, Alexandros Voliotis. An integrated maritime cyber security policy proposal. Available at: https://maritimecyberadvisors.com/_files/200000100-33f9a33f9d/MaritimeCybersecurityPolicy_v2.pdf, (2019)

[PAA16] European Commission, Paris Agreement. Document available at: https://ec.europa.eu/clima/policies/international/negotiations/paris_en, (2016).

[PAR15] Ioannis Parisis. The Maritime Dimension of European Security. Strategies, Initiatives, Synergies. Working paper Tufts University. Available at: https://sites.tufts.edu/karamanlischair/files/2018/12/KARAMANLIS-Working-Papers-2015-No-1.pdf, (2015).

[PIP20] Performance Improvements Partners. COVID-19 Cyber Security Statistics: 40 Stats And Facts You Can't Ignore. Available at: https://pip-llc.com/covid-19-cyber-security-statistics-40-stats-and-facts-you-cant-ignore/#finance, (2020).

[PWC20] PWC. Cyber Security in Shipping during COVID-19 pandemic. Available at: https://www.pwc.com/gr/en/industries/cybersecurity-in-shipping-industry.html, (2020).

[RED18] M. Reed, L. Oughton.: Stakeholders Analysis. SoilCare Scientific Report D3.1, Newcastle University (2018)

[SAF18] Safety4Sea, International Anti-Corruption Day: How shipping deals with high corruption levels. Available at: https://safety4sea.com/cm-international-anti-corruption-day-how-shipping-deals-with-high-corruption-levels/, (2018).

[SAF19] Safety4Sea, Top 10 issues concerning the future of shipping. Available at: https://safety4sea.com/cm-top-10-issues-concerning-the-future-of-shipping/, (2019)

[SEC20] Security Magazine. 70% of Organizations to Increase Cybersecurity Spending Following COVID-19 Pandemic, available at: https://www.securitymagazine.com/articles/92437-of-organizations-to-increase-cybersecurity-spending-following-covid-19-pandemic, last visited August, 2020.

[SEF19] European Commission. Spring 2019 Economic Forecast: Growth continues at a more moderate pace. Available at : https://ec.europa.eu/info/spring-2019-economic-forecast-growth-continues-more-moderate-pace_en, (2019) .

[SEF20] European Commission. Spring 2020 Economic Forecast: deep and uneven recession, an uncertain recovery. Online available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_799, (2020) .

[SLA14] M., Slabá.: Stakeholder Power-Interest Matrix and Stakeholder-Responsibility Matrix in Corporate Social Responsibility. 18th International Days of Statistics and Economics, available at: https://pdfs.semanticscholar.org/20f4/460b42e1fcb5f79f74e2c163c24367b91d88.pdf, (2014).

[SMC19] Maritime Knowledge. Safety management: Safety Culture vs Safety Climate – What's the difference? SAFETY4SEA article available at: https://safety4sea.com/cm-safety-management-safety-culture-vs-safety-climate-whats-the-difference/, (2019).

[TOP20] Tope Aladenusi. COVID-19's impact on Cybersecurity. Deloitte technical report, available at: https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html (2020).

[UFM20] Union for the Mediterranean. The maritime sector, an opportunity for development and growth in the Mediterranean. Available at: https://ufmsecretariat.org/the-maritime-sector-an-opportunity-for-development-and-growth-in-the-mediterranean/, consulted on May 2020.

[ZIO18] ZION Market Research. Blockchain in Energy Market: Global Industry Perspective, Comprehensive Analysis, and Forecast, 2017-2024. Available at: https://www.zionmarketresearch.com/report/blockchain-in-energy-market, (2018).

Annex 1: Cyber-MAR Ecosystem Questionnaire

Several EU projects are actively working in the research and development of cybersecurity solutions in the maritime domain. Table A1 compiles initiatives in which at least one Cyber-MAR partner is also involved. Table A2, refers to past EU projects related to cybersecurity and maritime areas.

Cybersecurity Ecosystem

NATIONAL CYBERSECURITY AUTHORITY	Name of the cybersecurity authority in your country. Also provide a link to the website
NATIONAL CYBERSECURITY STRATEGY	Name of the cybersecurity strategy in your country. Also provide a link to the website
IMPLEMENTATION DATE	Since when the cybersecurity strategy has been implemented?
BUDGET	How much is dedicated annually to this strategy?
FUNDING SOURCE	Where does the funding come from?
REGULATORY FRAMEWORK	Laws, regulations and any kind of legal document related to the cybersecurity strategy implemented in your country
MAIN ACTIVITIES PERFORMED	List of actions done by the cybersecurity authority in your country regarding the national strategy planned (200-250 words).
IMPACT TOWARDS NATIONAL CYBERSECURITY POSTURE	What is the expected impact of the cybersecurity strategy nationwide and internationally? (200-250 words)
BARRIERS AND CHALLENGES	What are the main challenges and barriers facing the cybersecurity agency while adopting the national cybersecurity strategy? (200-250 words)
IDENTIFIED NEEDS AND GAPS	What is missing or not well developed in your country in terms of cybersecurity? (200-250 words)
IDENTIFIED INITIATIVES IN CYBERSECURITY	List all major initiatives (e.g., projects, expert groups, events, etc) related to the cybersecurity domain
ADDITIONAL INFORMATION	Anything else to add?

Maritime Ecosystem

NATIONAL MARITIME INITIATIVES	List initiatives in the maritime domain currently adopted in your country.
WEBSITE LINKS	Provide a link to the website of each initiative
REGULATORY FRAMEWORK	Laws, regulations and any kind of legal framework related to the maritime strategy implemented in your country
MAIN ACTIVITIES PERFORMED	List of actions done in the maritime domain (200-250 words).
IMPACT TOWARDS NATIONAL POSTURE	What is the expected impact of the actions taken in the maritime domain? (200-250 words)
BARRIERS AND CHALLENGES	What are the main challenges and barriers facing the maritime domain in your country? (200-250 words)
IDENTIFIED NEEDS AND GAPS	What is missing or not well developed in your country in terms of shipping, ports and all related maritime aspects? (200-250 words)
ADDITIONAL INFORMATION	Anything else to add?