Assuring Cybersecurity on the Maritime Domain

Implementation of a Functional Organisation to Address the Cyber-security on the Maritime Domain

Sérgio Ricardo Caldeira de Carvalho

Thesis to obtain the Master of Science Degree in
Information Security and Cyberspace Law

Supervisor: Ph.D. Mário Monteiro Marques, EN
Ph.D. Richard F. Forno, UMBC
Ph.D. Carlos Lourenço Caleiro, IST

Examination Committee
Chairperson: Ph.D. Paulo Carreira Mateus, IST
Examiner: Rear Admiral António Gameiro Marques. ANS
Supervisor: Ph.D. Mário Monteiro Marques, EN

December 2019

Abstract

Information and communications technology (ICT) is revolutionising shipping, bringing with it a new era, the 'cyber-enabled' ship. Today's leading manufacturers and ship operators want to innovate using the latest ICT systems, going beyond traditional engineering to create vessels with enhanced monitoring, communication and connection capabilities, ships that can be accessed by remote onshore services, anytime and anywhere.

Also, the harbours are increasingly using digital technologies to handle and dispatch cargo in day to day operations. These new capabilities can bring a lot of commercial advantages and logistic gains, but they also raise a lot of security challenges.

In the current regulatory context for the maritime sector on global, regional and national levels, not much consideration has been granted to cybersecurity elements. Most security-related regulation only includes provisions concerning safety and physical security concepts, generally disregarding the digital threat to the sector.

With the promulgation of the new Portuguese cybersecurity law, which is a transposition of the EU Directive 216/1148, the crucial services that must be cyber protected are specified. Among them, are mentioned, in c) of point 2 of Annex II, the water transports, including inland, sea and coastal passenger and freight water transport companies, managing bodies of ports and the operators of vessel traffic services.

To be able to comply with this directive, it is necessary to define the security doctrine and to implement procedures to verify that all operators and digital services fully comply with all the requirements. In this work, we will study the design and implementation of a functional organisation that assures compliance to the directives on the water transports and maritime domain in general.

To do so, we will study the cybersecurity organisation in selected countries and in Portugal. Taking into account the results of this analysis, we will build a proposed model to apply to Portugal. Afterwards, we will validate it by conducting a survey to the key players on the maritime community and present the conclusions.

This work describes all the steps to construct a model that can have a practical use in Portugal and have a positive contribution to secure the Portuguese cyberspace of the maritime domain.

Resumo

As tecnologias de informação e comunicações (TIC) estão a revolucionar o transporte marítimo, trazendo consigo uma nova era, o "*navio digital*". Os principais construtores navais e operadores de navios querem inovar usando os mais recentes sistemas de TIC, indo além da engenharia tradicional para criar navios com capacidades aprimoradas de monitorização, comunicações e em rede, para que os navios possam ser acedidos e administrados por serviços remotos a partir das suas sedes em terra, a qualquer hora e em qualquer lugar que a plataforma se encontre.

Também os Portos utilizam cada vez mais as novas tecnologias para gestão e expedição da carga nas suas operações diárias. Essas novas capacidades trazem muitas vantagens comerciais e ganhos logísticos, mas também trazem muitos desafios de segurança.

No atual contexto regulatório para o setor marítimo ao nível global e nacional, há pouca consideração dada aos elementos de segurança do ciberespaço do setor. A maioria dos regulamentos relacionados com a segurança apenas inclui disposições relacionadas aos conceitos da proteção e segurança física, desconsiderando em geral a ameaça digital ao setor.

Com a promulgação, em Portugal, da nova lei de cibersegurança, que é uma transposição da Diretiva da UE 216/1148, especificam-se os serviços críticos em que deve ser garantida a sua cibersegurança. Entre eles, refere-se, na alínea c) do ponto 2 do anexo II, os transportes de marítimos, incluindo as empresas de transporte marítimo e costeiro de passageiros e mercadorias, as entidades de gestão portuária e os operadores de serviços de tráfego de embarcações.

Para poder cumprir esta legislação, é necessário definir a doutrina de segurança e implementar mecanismos necessários para verificar que todas as operadoras e serviços digitais cumprem integralmente todos os requisitos. Neste trabalho, estudaremos a conceção e implementação de uma organização funcional que garanta a conformidade das diretrizes no transporte de marítimo e no domínio marítimo em geral.

Para isso, estudaremos a organização de para a cibersegurança no domínio marítimo em países selecionados e em Portugal. Considerando os resultados dessa análise, iremos construir um modelo para aplicar em Portugal, validando-o através de inquérito conduzido aos peritos da comunidade marítima e apresentaremos as conclusões.

Este trabalho descreve todos os passos para construir um modelo que possa ser colocado em prática em Portugal e, assim, ter um contributo positivo para garantir a segurança do ciberespaço do domínio marítimo português.

Acknowledgements

Firstly, I would like to thank my supervisor, Professor Mário Monteiro Marques, and co-supervisor, Professor Richard F. Forno, for their guidance, patience and contribution to the successful completion of this thesis work.

My acknowledgements to the Navy´s Investigation Centre (CINAV), in the person of Director Professor Vítor Lobo, for the support and help in the development and research of the thesis, allowing me to have contact with different realities, a fact that had a paramount influence on the results.

My appreciation for the Portuguese Security Authority, and his staff, for their support.

My gratitude to Professor Filomena Teodoro for her help and support on the statistical analysis of the questionnaire results.

I want to thank the constant support of my loving wife Dulce and my son Afonso, for their love, motivation, patience and understanding that allowed me to meet this challenge.

Contents

Acronyms

A

ACPTMP	Autoridade Competente para a Proteção dos Transportes Marítimos e Portos (Competent Authority for the Protection of the Maritime Transports and Ports)
AD	Attaché de défense
AEM	Action de l'État en mer
AIP	Administração das Instalações Portuárias (Port Facilities Administration)
AMN	Autoridade Marítima Nacional
AMSC	Area Maritime Security Committees
AMSP	Area Maritime Security Plan
ANSSI	Agence nationale de la sécurité des systèmes d'information
ANT	Actor-Network Theory
AODM	Activity-Oriented Design Method
APP	Autoridade de Proteção Portuária (Port Protection Authority)
ASI	Attaché de sécurité intérieure
ASP	Agents de sûreté portuaire
AMT	Autoridade da Mobilidade e dos Transportes

B

BSL	Brigade de surveillance du littoral

C

CapINav	Capacité nationale de renfort pour l'intervention à bord des navires
CCE	Cellule de continuité économique
CCIM	Cellule de coordination de l'information maritime
CCN	Centro Criptológico Nacional
CCOPP	Coordination Centre for the Security Operations
CCPP	Comité Consultivo para a Proteção Portuária (Consultee Committee for the Port Security)

CCPTMP	Consultee Council to the Protection of the Maritime Transport and Ports
CEMAS	Cellule d'évaluation des menaces et d'analyse de sûreté
CEO	Chief Executive Officer
CERT	Crisis Emergency Response Team
CERTSI	Centro de Respuesta a Incidentes de Seguridad de la Información
CES	Comité Especializado de Situación
CESG	National Technical Authority for Information Assurance
CFP	Cybersecurity Framework Profile
CG-791	Office of Cyberspace Forces
CGGD	Commandant de groupement de la gendarmerie départementale
CI	Critical Infrastructures
CIC	Cellule interministérielle de crise
CII	Critical Information Infrastructures
CIMer	Comité interministériel de la mer
CIP	Critical Infrastructure Protection
CISMaP	Commission interministérielle de sûreté maritime et portuaire
CISO	Chief Information Security Officer
CiSP	Cardholder Information Security Program
CLSP	Comité local de sûreté portuaire
CMSE	Chargé de mission de sécurité économique
CNC	Consejo Nacional de Ciberseguridad
CNCS	Centro Nacional de Ciberdefesa (National Centre for Cybersecurity)
CNI	Critical National Infrastructures
CNN	National Coordination Council
CNS	Centres de Sécurité des Navires
CNPIC	Centro Nacional para la Protección de las Infraestructuras Críticas
CNRLT	Coordination nationale du renseignement et de la lutte contre le terrorisme
CNSM	Centre national de la sécurité des mobilités
COBR	Cabinet Office Briefing Rooms
CoFIS	Comité de la filière des industries de sécurité
COM	Centre des Opérations Maritimes
ComGendMar	Commandement de la gendarmerie maritime
COMIA	Commandant interarmées
COMSUP	Commandant supérieur
CoNPIC	Comisión Nacional para la Protección de las Infraestructuras Críticas
CORGMar	Centre d'opérations et de renseignement de la gendarmerie maritime
COSSI	Centre opérationnel de sécurité des systèmes d'information de l'ANSSI
COTP	Captain of the Port
COTS	Commercial of the Shelf

CPNI	Centre for the Protection of National Infrastructure
CRGN	Commandant de région de la gendarmerie nationale
CRMar	Centre de renseignement de la Marine
CROGEND	Centre de renseignement opérationnel de la gendarmerie
CROGMar	Centre de renseignement et d'opérations de la gendarmerie maritime
CROSS	Centre régional opérationnel de surveillance et de sauvetage
CRZGN	Commandant de région de la zone de gendarmerie nationale
CS Officer	Cybersecurity Officer
CS&C	Office of Cybersecurity and Communications
CSA	Cybersecurity Assessment
CSF	Cybersecurity Framework
CSI	Container Security Initiative
CSIRT	Computer Security Incident Response Team
CSN	Consejo de Seguridad Nacional (National Security Council)
CSO	Company security officer
CSOC	Cyber Security Operations Centre
CSP	Cybersecurity Plan
CySO	Cybersecurity Officer
CZGN	Commandant de zone de la gendarmerie nationale
CZM	Commandant de zone maritime

D

DAM	Direction des affaires maritimes
DCO	Deputy Commandant for Operations
DDG	Délégué du gouvernement
DDPAF	Directeur départemental de la police aux frontières
DDRT	Directeur départemental du renseignement territorial
DDSP	Directeur départemental de la sécurité publique
DfT	Département for Transports
DGAM	Direção-Geral da Autoridade Marítima (General Direction of the Maritime Authority)
DGGN	Direction générale de la gendarmerie nationale
DGITM	Direction générale des infrastructures, des transports et de la mer
DGMM	Dirección General de la Marina Mercante
DGRM	Direção-Geral dos Recursos Naturais, Segurança e dos Serviços Marítimos (General Direction of the Natural Resources, Safety and Maritime Services)
DGSE	Direction générale de la sécurité extérieure
DGSI	Direction générale de la sécurité intérieure
DHS	Department of Homeland Security

DIRD	Directeur interrégional des douanes
DMT	Défense maritime du territoire
DNRE	Direction nationale du renseignement et des enquêtes douanières
DNS	Directive nationale de sécurité
DPSA	Dispositif particulier de sûreté aérienne
DPSM	Dispositif particulier de sauvegarde maritime
DRB	Détachement renfort Bretagne
DRM	Direction du renseignement militaire
DRRI	Direction régionale du renseignement intérieur
DRSD	Direction du renseignement et de la sécurité de la défense
DSN	Situation Centre of the National Security Department
DSP	Digital Service Providers
DST	Direction des services de transport
DSûT	Département de la sûreté dans les transports

E

EDIM	Équipes de défense et d'interdiction maritime
EMA	État-major des armées
EMM	État-major de la marine
ENCS	Estrategia Nacional de Ciberseguridad
ENISA	European Network and Information Security Agency
ENS	Estrategia de Seguridad Nacional (National Security Scheme)
EO	Executive Order
EP3R	European Public-Private Partnership for Resilience
EPE	Équipe de protection embarquée
EPNAP	Équipes de protection des navires à passagers
EPPN	Équipe privée de protection des navires
ESIP	Évaluation de sûreté de l'installation portuaire
ESP	Évaluation de sûreté du port
EU	European Union
EWS	Early Warning System

F

FBI	Federal Bureau of Investigation
FGC	Fonction garde-côtes
FSA	Facility Security Assessment
FSP	Facility Security Plans

G

GCHQ	Government Communications Headquarters
GIR marine	Groupe d'intervention rapide de la marine
GISTMOP	Groupe interministériel de sûreté du transport maritime et des opérations portuaires
GMar	Gendarmerie maritime
GNS	Gabinete Nacional de Segurança (Portuguese Security Authority Cabinet)
GPD	Groupe de plongeurs démineurs
GVA	Gross Value Added

H

HFDS	Haut fonctionnaire de défense et de sécurité

I

ICS-CERT	Industrial US Computer Emergency Readiness Team
ICT	Information and Communications Technology
IET	Institution of Engineering and Technology
IMO	International Maritime Organisation
IP	Installation portuaire
IPD	Installation prioritaire de défense
ISAC	Information Sharing and Analysis Centre
ISM	International Safety Management (Code ISM)
ISPS Code	International Ship and Port Facility Code
ISPS	International Ship and Port Facility Security (Code ISPS)
ISSC	International Ship Security Certificate
IT	Information Technology

L

LGD	Lead Government Department
LPS	Limites portuaires de sûreté

M

MASA	Mesures actives de sûreté aérienne
MBLT	Maritime Bulk Liquids Transfer
MCA	Maritime and Coastguard Agency
M-CERT	Maritime CERT
MD	Maritime Domain
MICA centre	Maritime Information Cooperation and Awareness centre

MOD	Ministry of Defence
MSC	Maritime Safety Committee
MSRAM	Maritime Security Risk Assessment Model
MSSMB	Maritime Security and Safety Management Branch
MTS	Maritime Transport System
MTSA	Maritime Transportation Security Act

N

NCC	National Coordinating Centre for Communications
NCCIC	National Cybersecurity and Communications Integration Centre
NCSC	National Cyber Security Centre
NCSC-NL	Netherlands National Cybersecurity Centre
NCSP	National Cyber Security Program
NEDEX	Neutralisation, enlèvement, destruction des explosifs
NIPP	National Infrastructure Protection Plan
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NMSC (I)	National Maritime Security Committee (Industry)
NO&I	NCCIC Operations and Integration
NPPD	National Protection and Programs Directorate
NRA	National Risk Assessment
NSAR	National Suspicious Activity Reporting
NSC	National Security Secretariat
NSMS	National Strategy for Maritime Security

O

OCMI	Officer in Charge Maritime Inspections
OCSIA	Office of Cyber Security & Information Assurance
OES	Operator of Essential Services
OIV	Opérateur d'importance vitale
OMI	Organisation maritime Internationale
OPC	Oficial de Proteção da Companhia (Company Security Officer)
OPIP	Oficial de Proteção das Instalações Portuárias (Officer of Security of the Ports Facilities)
OSH	Organismes de Sûreté Habilités

P

PCA	Plan de continuité d'activité
PFSA	Port Facility Security Assessment

PFSA	Port Facilities Security Assessment
PFSO	Port facility security officer
PFSP	Port Facilities Security Plan
PIV	Point d'importance vitale
PM	Polícia Marítima (Maritime Police)
PNR	Passager Name Record
PPE	Plan de protection externe
PPP	Plan particulier de protection
PPP	Public-Private Partnership
PSA	Port Security Authority
PSC	Port Security Committee
PSI	Proliferation security initiative
PSIP	Plan de sûreté de l'installation portuaire
PSMP	Peloton de sûreté maritime et portuaire
PSO	Plan de sécurité d'opérateur
PSO	Port Security Officer
PSP	Plan de sûreté portuaire
PSP	Port Security Plan
PWSA	Ports and Waterways Safety Act of 1972
PZDS	Préfet de zone de défense et de sécurité

S

SAIV	Sécurité des activités d'importance vitale
SAM	Sistema de Autoridade Marítima
SCADA	Supervisory Control and Data Acquisition
SCySO	Ship Cybersecurity Officer
SDAO	Sous-direction de l'anticipation opérationnelle
SDRT	Service départemental du renseignement territorial
SDSIE	Service de défense, de sécurité et d'intelligence économique
SGDSN	Secrétariat général de la défense et de la sécurité nationale
SGMer	Secrétariat général de la mer
SGSCIM	Subdirección General de Seguridad, Contaminación e Inspección Marítima
SHFD	Service du haut-fonctionnaire de défense (MININT)
SHFDS	Service du haut fonctionnaire de défense et de sécurité
SMC	Secteur maritime côtier
SNSEM	Stratégie nationale de sûreté des espaces maritimes
SNSM	Société nationale de sauvetage en mer
SOC	Security Operations Centre
SOLAS	Safety of Life at Sea (Convention SOLAS)

SPR	Secteur de protection rapprochée
SRGMar	Section de recherches de la gendarmerie maritime
SRRT	Service régional du renseignement territorial
SSA	Sector-Specific Agencies
SSA	Ship Security Assessment
SSMUE	Stratégie de sûreté maritime de l'Union européenne
SSO	Ship security officer
SSP	Ship Security Plan

T

TA	Activity Theory

U

UCLAT	Unité de coordination de la lutte antiterroriste
UE	Union européenne
UK	United Kingdom
ULAM	Unité littorale des affaires maritimes
USA	United States of America
US-CERT	US Computer Emergency Readiness Team
USCG	United States Coast Guard

Z

ZPS	Zone portuaire de sûreté
ZRP	Zone de responsabilité permanente

List of Figures

List of Tables

1

Introduction

This chapter aims to present the motivation for this work, the research question and the hypotheses generated by this question, the research method used, the contributions of this thesis and the structure it follows.

1.1. Motivation

Cyberspace has brought an enormous number of opportunities for development in all fields, from economics to science and even military development. But with all these opportunities, it has also created a lot of security challenges.

Security is a critical function for an organisation, company, agency or unit. Consequently, security is implemented to protect critical assets of all types, ranging from staff, equipment and facilities to computerised systems. Security implementations themselves are assets, requiring the same security protections that they, in turn, offer to the broader organisation. Most organisations claim they understand the need for protecting and monitoring cyber-linked business support and control systems. Even so, the breadth and complexity of protecting such systems may present a daunting challenge to many organisations that do not have a comprehensive picture of cybersecurity [1].

Successful cybersecurity is the result of a complex series of related and interdependent work efforts that combine to provide protections that are functional and enduring against challenges presented by geography, technological evolution, and shifting human resource capabilities and deployment [1].

Information and communications technology (ICT) is revolutionising shipping, bringing with it a new era: the ‘cyber-enabled’ ship. Today’s leading manufacturers and ship operators want to innovate using the latest ICT systems, going beyond traditional engineering to create vessels with enhanced monitoring, communication and connection capabilities, ships that can be accessed by remote onshore services, anytime and anywhere [2].

The ICT systems have the potential to improve safety, reliability and business performance, but the need remains to identify numerous risks, understand and mitigate them to make sure that technologies are safely integrated into ship design and operations. The marine industry faces complex and severe challenges to guarantee the benefits of using these technologic systems.

Since a modern digital-based ship consists of multiple, interconnected systems, and because of the rapid pace of technology development, assuring that a cyber-enabled vessel will be safe cannot be prescriptive, and cannot rely on knowledge gained from previous systems. Instead, it requires a 'whole systems' approach, one that takes account of all the different systems on-board and onshore, how they are designed, installed and operated, how they connect and how they will be managed.

Also, Ports play a crucial role at different levels for many sectors and have been successful pioneers in Europe for interconnecting the different types of transport. As the main channel for imports and exports (food, commodities, etc.) to the rest of the world, ports also enable trade and contacts between all nations. Moreover, ports are important nodes for passengers and vehicles transportation, and they play a key role in fishing activity [3].

For several years, ports have been undergoing a digital transformation in order to meet emerging challenges, optimise existing processes and introduce new capabilities, such as automation and real-time monitoring of operations. This digital transformation has also led to a change in the sector's cyber risk profile, as shown in the proliferation of cybersecurity incidents in ports over the past few years, such as the cyberattack in Antwerp port, the NotPetya Ransomware incident and its impact on Maersk and the wave of ransomware attacks in Ports of Barcelona and San Diego [3].

In the current regulatory context for the maritime sector on global, regional and national levels, not much consideration has been granted to cybersecurity 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) N. º 725/2004 on enhancing ship and port facility security. These regulations do not consider cyber-attacks as possible threats of unlawful acts.

With the promulgation of the new Portuguese cybersecurity law (Law 46/2019, of 13 August) [4], that is a transposition of the EU Directive 216/1148, the role of the Portuguese National Cybersecurity Authority to assure the security of the Portuguese Cyberspace is reinforced. This law specifies the essential services that must be cyber protected, among them are mentioned, in c) of point 2 of Annex II, the water transports, including inland, sea and coastal passenger and freight water transport companies, managing bodies of ports and the operators of vessel traffic services. To be able to comply with this directive, it is necessary to define the security doctrine and to implement procedures to verify that all operators and digital services fully comply with all the requirements. In this work, we will study the design and implementation of a functional organisation that assures compliance with the directives on the water transports and maritime domain in general.

It is necessary to create a functional model that not only allows the verification of the compliance of the cybersecurity standards on the maritime domain but also defines the framework of the standards and the way to promulgate them, establishing routines of inspection to verify their implementation by the marine community.

The Maritime Authority System (SAM) has an essential role to perform in this task, being part of the solution for a cyber safer maritime domain. So, it is urgent for one of the SAM organisms to

take charge of this task and start to develop and implement the procedures to avoid a lack of control and to prevent fragilities on the cybersecurity of the strategic national area of the water transportation sector.

The need of a functional organisation to assure the cyber safety of the maritime domain is not new, and there are very successful examples of sound and effective cybersecurity models at work in countries as the United States, the United Kingdom, Germany, Spain, France, among others.

Also, the doctrine and procedures concerning maritime cybersecurity are already mostly done. International organisations like IMO and BIMCO spread good practice recommendations and processes, many reverted to a national doctrine like IED did in the UK.

It is necessary to assess if any of these existing models are directly applicable to Portuguese reality, if there is the need to adopt one specific model, or if we can build a new one based on the ones already implemented, adapting the best of each to Portuguese standards and capabilities.

Concerning the doctrine, the publications and standards that already exist, in several trustable sources, should be adapted to comply with the European Directives, the International Law and the Portuguese National Law. There is no need to develop a new doctrine but only to suit the existing one.

Standardisation will always be the final objective, to facilitate the international institutional relationship and to harmonise the requirements allowing the ship handlers to have the same requirements regarding the cybersecurity in all the harbours that ships practice and operate from, improving the maritime business model and increasing the maritime cybersecurity.

1.2. Research Question

There is the need to create and implement an organisational and a procedural model to ensure cybersecurity in the Portuguese maritime domain and to verify that the national law of cybersecurity is followed and implemented by the maritime community.

Therefore, the main research question chosen for this work is the following:

What is the organisational model for assuring the cybersecurity in the Portuguese Maritime Domain and ensuring the Cybersecurity Law compliance?

To answer the main research question, I propose to prove the following four hypotheses:

H 1 – *The European organisational models to assure the cybersecurity in the maritime domain are more adequate for the Portuguese reality than others.*

H 2 - *The EU legislative framework has more influence on the adopted model to ensure cybersecurity in the EU countries than the other factors*.

H 3 – *Adapting the actual maritime domain security organization so as to include the cybersecurity aspect is more efficient and quicker to implement than raising a completely new organisation*.

H 4 - *The leading entity to coordinate the cybersecurity in the maritime domain should be an organism specialised in the Maritime Domain with a cybersecurity background and an established cybersecurity organisation rather than other with no cybersecurity experience or expertise*.

1.3. Research Method

The research method used is a classical approach, and it comprises several steps [5]. The process is represented in Figure 1-1 and then explained in the following paragraphs.

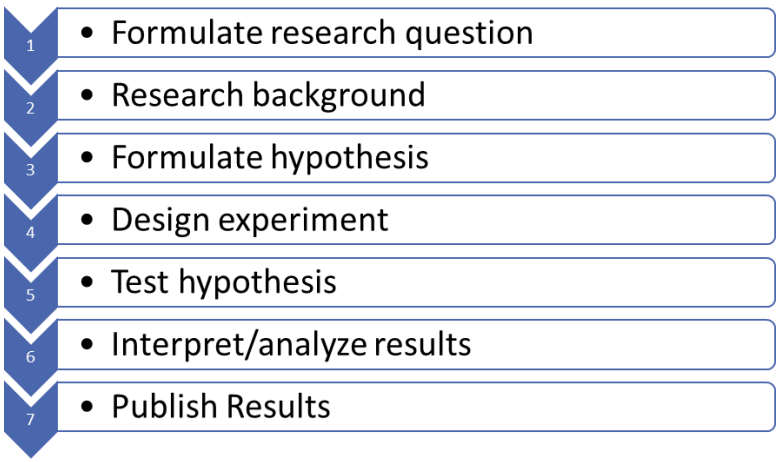


Figure 1-1 - Research Method

The first step of research is to formulate the research question based on the problem it proposes to study or to resolve.

Research background is the second step of the proposed research method. It should be comprehensive, that is based on extensive research on the subject or other related areas. It is an essential step of the method, since it makes the following steps easier.

Based on the information gathered on the previous step, the third step consists of formulating the hypothesis which the researcher considers to be the solution to the problem identified in the research question. However, this step is not meant to develop the answer, which will only be fully exploited in the next step, design experiment. For example, if the resolution of a specific problem involves adapting a UK structure to Portugal, this is not analysed in the formulation of the hypothesis, but on the following step.

As was mentioned before, the fourth step consists in designing the experiment, it is the practical phase of the research, and it often involves outlining an organisational structure, developing a particular procedure, or other solutions.

The fifth step is to test the hypothesis, collecting data. It is essential to evaluate the organisational solutions, the developed procedures and the publications. To do so, we will ask the opinion of experts on cybersecurity in the maritime domain.

After gathering all the answers of the experts, we should interpret the results and analyse them in order to validate the proposed solution. However, if the results are not satisfactory, it is possible to return to step 3, the formulation of a new hypothesis.

The method used to test the hypothesis will be to conduct a questionnaire in order to ascertain the acceptance of the proposed solution by the maritime community.

1.4. Conducting the research background analysis

To study the results obtained in the background research, we will use a model that combines three well known theoretic baselines: one based on strategy, Grand Strategy; another on the activity system interpretation, the Activity Theory (TA); and the third one on the Actor-Network Theory (ANT), that is broadly used in new technology research.

The combined model of these three theories will help us understand the organisations devised by the countries to tackle the cybersecurity issue and will allow us to adopt, adapt or design a model applicable to Portugal.

1.4.1. Grand Strategy Theory

One of the grand strategic studies of reference is the *Strategic Theory for the 21st Century: The Little Book on Big Strategy*, by Harry R. Yarger [6].

Strategic planning is an inherently human activity focused on root, purposes and causes, and a good strategy is both practical and efficient, but effectiveness takes precedence over efficiency [6].

Strategy is a method of creating effects favourable to policy and interests by defining the **ends, ways, and means** in the strategic sphere, seeking «a synergy and symmetry of objectives, concepts, and resources to increase the probability of policy success and the favourable consequences that follow from that success». Thus, valid strategies include ends, ways, and means that lead to the accomplishment of the desired end state within acceptable bounds of feasibility, suitability, acceptability, and risk [6].

- **Objectives (ends)** specify "what" is to be accomplished and are limited by policy guidance, higher strategy, the nature of the strategic environment, the capabilities and limitations of the instruments of power of the state, and resources made accessible. Objectives are expressed with explicit verbs.
- **Strategic concepts (ways)** answer the question of "how" the objectives are to be achieved by employing the instruments of power. They link resources to the objectives by designating who does what, where, when, how, and why, with the responses to which explaining "how" an objective will be achieved.
- **Resources (means)** in strategy formulation set the boundaries for the types and levels of support modalities that will be made available for pursuing concepts of the strategy, and they can be tangible or intangible.

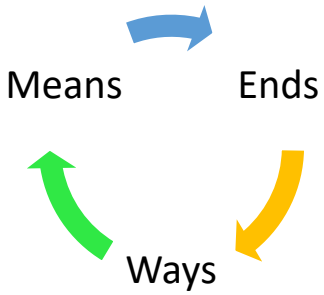


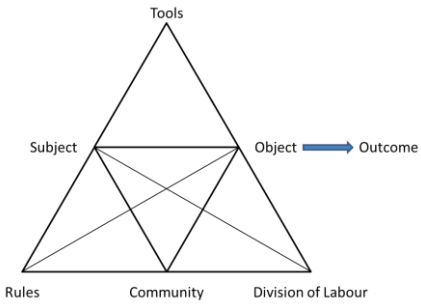
Figure 1-2 - Strategy Cycle

Strategy has an inherent logic of **suitability, feasibility, and acceptability**. Will the attainment of the objectives give us the strategic effects that we seek for? (**Suitability**). Do those strategic effects justify the objectives pursued and the methods and resources used to achieve them? (**Acceptability**) Are the strategic ends achievable with the resources available? (**Feasibility**). [6] Risk is determined through an assessment of the probable consequences of success and failure.

1.4.2. The Activity Theory

Activity Theory is a philosophical and cross-disciplinary framework for studying different forms of social practices as development processes with both individual and social levels interlinked at the same time. [7].

Activity Theory has evolved through three generations of studies. The first generation involves the work of Vygotsky, who argued that humans' interactions with their environments are indirect or mediated [8]. The second generation of AT is based on Leontiev's work [9], which states that the activity system is the basic unit of analysis, even though it includes several components. [10]



Components	Description
Subject	It is the individual or group of actors engaged in the activity
Tools	It can be anything used in the transformation process (i.e. like cutter or computer mouse)
Object	Object can be any tangible or intangible things such as plans or even creative ideas
Outcome	The expected result or the goal that the activity try to achieve
Division of Labour	It refers to vertical power of status and how tasks are split horizontally between community members.
Community	It negotiates and mediates the rules and customs that describe how the community functions
Rules	It is the norms, traditions, or laws that exist in particular communities.

Figure 1-3 - Components of Activity System [10]

The components include [11]:

- Tools – physical or psychological entities, including signs, procedures, machines, methods or laws. Tools mediate subject activity towards the object and they are used by subjects when performing activities.
- Subject – technical and non-technical entity engaged in activity operations. The subject is the agent who acts upon the object of the activity. A subject can be referred to as an individual or group of actors who perform an activity.
- Object – material thing, or less tangible and even intangible element (e.g. idea) that those involved in an activity can share. An activity is directed to an object which motivates an operation.
- Community – interdependent gathering of individuals who share a set of social meanings. We can define a community as a social group within which the subject is identified while participating in an activity.
- Rules – activities are carried out in communities bounded by rules, in an analysis of activities, different kinds of rules, laws, norms and cultural practices. Rules govern subjects as they carry out their activities and interactions with other elements of the community. Thus, on the one hand, rules are necessary for maintaining order in communities; on the other hand, they can, in varying degrees, constrain or allow an activity.
- Division of labour – allocation of specific tasks to individuals by areas of specialisation. Division of labour is concerned with how responsibilities are divided between community members and how power and status are distributed in an environment. Division of labour is crucial, as this enables the sharing of activities among community members, each subject being assigned a particular responsibility.

- Outcome – results of the activity. Each component of the AT significantly contributes and has an impact on the outcome of an activity within a social system. The effect can be positive or negative, depending on the situation of the phenomenon being studied or the environment where the activity was carried out.

An activity produces outcomes and is performed through actions. Nevertheless, the activity cannot be reduced to actions. Individual actions are linked to specific targets or goals. Actions are performed through operations. Operations are performed in an autonomous way, not clearly related to goals [12]. Operations depend on the conditions in which actions are performed. [7] In this context, an activity has a structure of three levels: Activity, Action and Operation [13, 8].

Table 1-1 - Structure of an Activity [13]

Level	Description	Question
ACTIVITY	The smallest milieu that allows to understand the effort done buy a collection of people to attain a collective result	Why things happen?
ACTION	Can only be understood in the context of the activity	What is it made of?
OPERATION	The means used to implement the actions conditions	How is this done?

- An activity is understood as a chain of individual and supportive actions. The actions related to an activity are connected by the same objective and motive;
- Actions contribute to the activity. They have a goal, which can only be understood in the context of the corresponding activity;
- Operations are well-defined routines used subconsciously as responses to conditions faced during the performing of the action.

The third generation AT, more commonly known as Cultural Historical Activity Theory (CHAT) [14], expands the unit of analysis from one activity system to at least two interacting activity systems as the smallest unit of study [10].

In our analysis, we will use the AT of the 2nd Generation. AT provides a philosophical framework for comprehending collective human work activities as embedded within a social practice (e.g. an organisation) and mediated by artefacts. [15] AT supports the concept of decomposing a complex activity during analysis in order to have a detailed understanding of the nature of work and responsibilities of those involved in the activity. Also, it is object-oriented; this means that every activity is directed towards some object. Another crucial aspect is that different kinds of rules, laws, norms and cultural practices of the environment or community in which activity occurs must be taken into consideration in the analysis of AT's activity system. [10]

Several AT based models have been developed, but the model we will give special attention is the Activity-Oriented Design Method (AODM) [16] that was proposed by Mwanza and is based on the models of Engeström. Mwanza created the Eight Steps Model, which is useful to identify the components of the activity system.

Table 1-2 - Mwanza's Eight Steps Model [13]

Identify	Question to ask
Subject	Who is involved in carrying out this activity?
Objective	Why is the activity taking place?
Subjects	Who is involved in carrying out this activity?
Tools	By what means are the subjects performing this activity?
Rules and Code	Are there any cultural norms, rules or regulations governing the performance of this activity?
Division of labour	Who is responsible for what, when carrying out this activity and how are the roles organized?
Community	What is the environment in which this activity is carried out?
Outcome	What is the desired *Outcome* from carrying out this activity?

In this analysis, we can see the influence that the legal framework has on the subjects, on the tool's usage, on the community and consequently on the output of the organisation. Thus, we can state that the legal framework has a crucial role in the organisational structure and outcome.
All countries taken into consideration here will be subjected to an Activity Theory analysis.

1.4.3. The Actor-Network Theory (ANT)

ANT considers "science and technology in the making" as opposed to "readymade science and technology" [17]. ANT attempts to "open the black box" of science and technology by tracing the multifaceted relations that exist between governments, technologies, knowledge, texts, money and people. These are the connections that result in science and technology, and by examining them, it becomes easier to describe why and how we have the science and technology that we do. [18]
ANT suggests that any system we encounter can most effectively be approached if we look at all the parts, whether natural, technological, or human, like interrelating and active members of the system. ANT states that each human being, each piece of technology, and each natural factor has an identical role in the system and must be considered and that every event that occurs may be mentioned as a network (a group of elements that interconnect and affect each other), composed of actants (parts of the network that have some role to play) and connections (ways in which the components interact) [19].
Going through the basic concepts of this theory we will start with the actants (the semiotic definition of an actor in this theory), meaning those who act or to whom or which activity is granted by another and can be anything, provided it is allowed to be the source of action. [19]
So, according to ANT, all actants are supposed to be equally essential participants; actants are measured and valued only by how they interact in the system: intermediaries are actants that do not tend to change the system and mediators are actants that do cause changes in the system.
For ANT a network is always an actant-network, it is simultaneously an actor whose activity is networking heterogeneous elements and a network that can redefine and transform what it is made of. Everything can be considered both an actor and a network, and it is merely a matter of perspective [18]. Actant-networks are thus constructed and reconstructed through interaction between actants. [20] If the actants keep interacting, the actant-network will look stable from the outside.

ANT argues that both human and non-human actors are comprehended inside a network, their identity being defined through their interaction with other actors; this is called generalised symmetry [21]. The differences between humans and nonhumans are not neglected but they have no a-priori relevance for ANT driven research.

According to this theory, we are not primarily concerned with mapping interactions between individuals, we are more interested in mapping how they, actors, define and distribute roles and mobilise or invent others to play these roles. [22]

The interaction between actants is necessary to establish and hold the connections between them. For the actants to build relationships, they must be displaced and transformed in order to make them fit into an actant-network. The work that is necessary to displace and transform is called translation.

For ANT, translation is understood as all the negotiations, intrigues, calculations, acts of persuasion and violence through which an actant is changed. Translation is a concept that bridges the gap between the varied aspects that are combined in technology; it involves creating convergences and homologies by relating things that were previously different [23]. If there are uncountable entities and meanings built into technology, translation is the process by which these elements are related in a sociotechnical network, the method by which the identification of the actors, the likelihood of interaction and the margins of manoeuvre are negotiated and delimited [24]. When actants have not been translated (or translate themselves), they are not part of the actant-network. [18]

Interaction is like a flow: something flows from one actor-network to another. ANT driven research wants to track these flows. The research starts from the chosen actant and then begins by exploring and unravelling this actant and the human and non-human actants that relate to it. [19]

For ANT, to study any organisation, social order, technical innovation or scientific discovery is to explore the connections between heterogeneous actors joined within a network [18].

ANT is one of the most used theories to analyse the technological, social field.

1.4.4. The analysis model created

The model established to investigate the problem and justify the proposed solution is based on the Grand Strategy, the Activity Theory and the Actor-Network-Theory.

The problem can easily be addressed within the frame of these three theories, and I will use it to create the model for analysing the organisational structure of the reference countries.

An assumption that must be made is that the analysis of these organisational structures is not to find an organisation to implement in Portugal, but to know the rationale and the approach made by these countries to create their organisational and doctrinaire structure regarding the cybersecurity on the maritime domain. Nevertheless, the proposed model to be applied in Portugal will include the adaptation of good practices and the publications that are already promulgated in those countries concerning this issue.

The Grand Strategy approach gives us a solid doctrinal basis, the final goal of the organisational structure being the state policy objective of assuring the cybersecurity of a critical national sector, the maritime transportation. The strategy is subordinated to the policy, so, in the end, what we want is a strategy to assure the cybersecurity on the maritime domain. Therefore, we can analyse

these countries' organisation concerning the End, the Ways and the Means to achieve cybersecurity in the maritime domain; this involves defining what strategy they follow, what means they use (including the functional organization to implement it), and what resources they employ to assure it.

To be able to conduct a more in-depth analysis of these organisations considering the entire work/activity system (including teams, organisations, etc.) it was essential to have a framework that could offer the constant evaluation of a statement of requirements. That framework could be found in the Activity Theory, which accounts for the environment, history of the person, culture, role of the artefact, motivations, and complexity of the real-life action. The unit of study in AT is the concept of object-oriented, collective and culturally mediated human activity, or activity system. An activity is a goal-directed or purposeful interaction of a subject with an object using tools. These tools are exteriorised forms of mental processes manifested in constructs, whether physical or psychological. The AT recognises the internalisation and externalisation of cognitive processes involved in the use of tools, as well as the alteration or development that results from the interaction [25].

Considering the definitions made of Ends, Ways and Means [6], and crossing them with the meaning of Objectives, Tools, Subject, Rules, Community, Division of Labour and Outcome and the Mwanza's Eight Steps Model [11], we can derive the following relation:

Table 1-3 - Relationship between Grand Strategy and AT

Gran Strategy [4]	Activity Theory [17]
Ends **Explain "what" is to be accomplished**	Objective Why is the activity taking place?
	Outcome What is the desired Outcome from carrying out this activity?
Ways **Answer the big question of "how" the objectives are to be accomplished**	Rules Are there any cultural norms, rules or regulations governing the performance of this activity?
	Division of Labor Who is responsible for what, when carrying out this activity, and how are the roles organised?
	Community What is the environment in which this activity is carried out?
Means **Set the boundaries for the types and levels of support modalities that will be made available**	Tools By what means are the subjects performing this activity?
	Subjects Who is involved in carrying out this activity?

In a first generic approach for the TA will be the following:

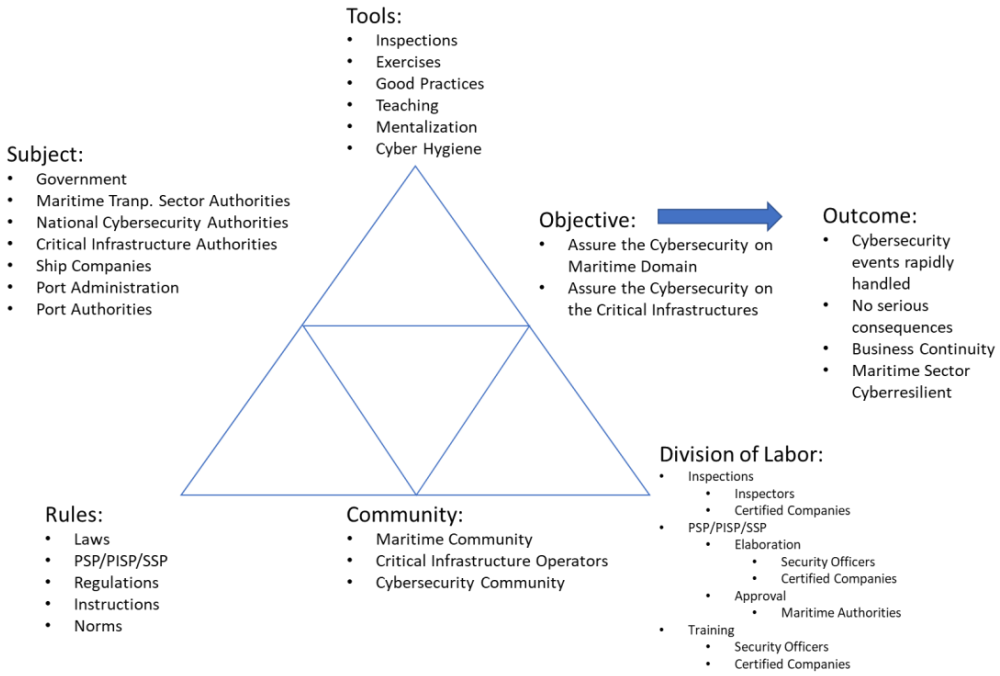


Figure 1-4 - First generic approach for the TA on Cybersecurity on Maritime Domains

To introduce the ANT in this analysis model, first we will make a comparison with the Grand Strategy. We can consider that Ends, Ways and Means are mediator actants because they can all induce changes in the system. The Ends affect the Ways needed and they depend on the Means to be executed. So, in this actant-network, the actants interconnect keeping the stability of the network. If the stability of this actant-network is compromised, the interaction between actants starts to fail and the risk of not achieving the goal increases.

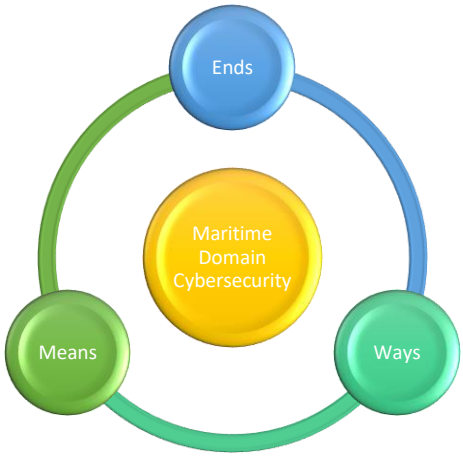


Figure 1-5 - The Grand Strategy

After having established the relation between the Grand Strategy and AT done, we will now make the connection with the ANT. So, as previously explained in Table 1-3:

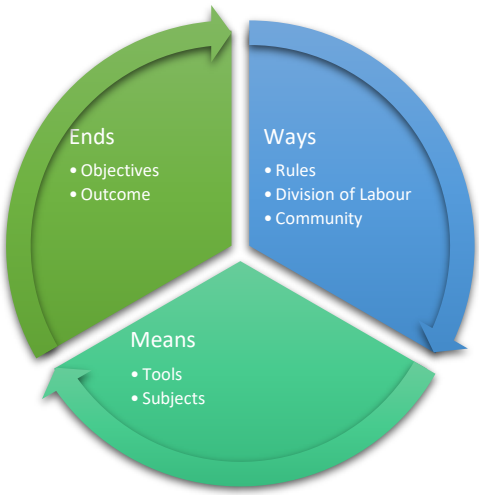


Figure 1-6 - Relationship between Grand Strategy and AT

In this stage of the ANT, we can consider that these actants belong to different types: some are mediators and others are intermediates. This is the case with Objectives and Outcomes: the former have an influence on the network which pervades all actants of the network; the latter, on the contrary, are a result of the network, which means that even when outcomes changes this will have no bearing on the other actant mediators, that can continue their interactions unaffected: even if those interactions change in nature or objective, they will continue and the network will remain stable. For model purposes, these are the results assumed considering the actants types:

Table 1-4 - Relationship between Grand Strategy, AT and ANT

Grand Strategy	TA	ANT	
		Mediators	Intermediates
Ends	Objectives Outcome	Objectives	Outcome
Ways	Rules Division of Labour Community	Rules Division of Labour	Community
Means	Tools Subjects	Tools	Subjects

This first level of ANT may be represented by the following diagram:

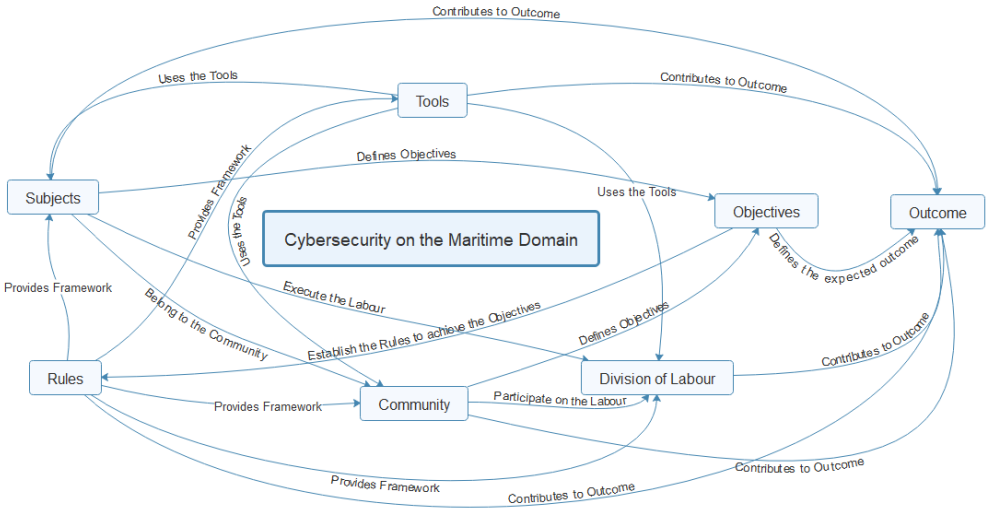


Figure 1-7 - ANT Generic 1st Level

We could move on to the second level of ANT, decomposing all the elements of each actant of the first level and so forth until we reached the detailed level required.

To integrate the mentioned theories in a single view, we could present the following diagram:

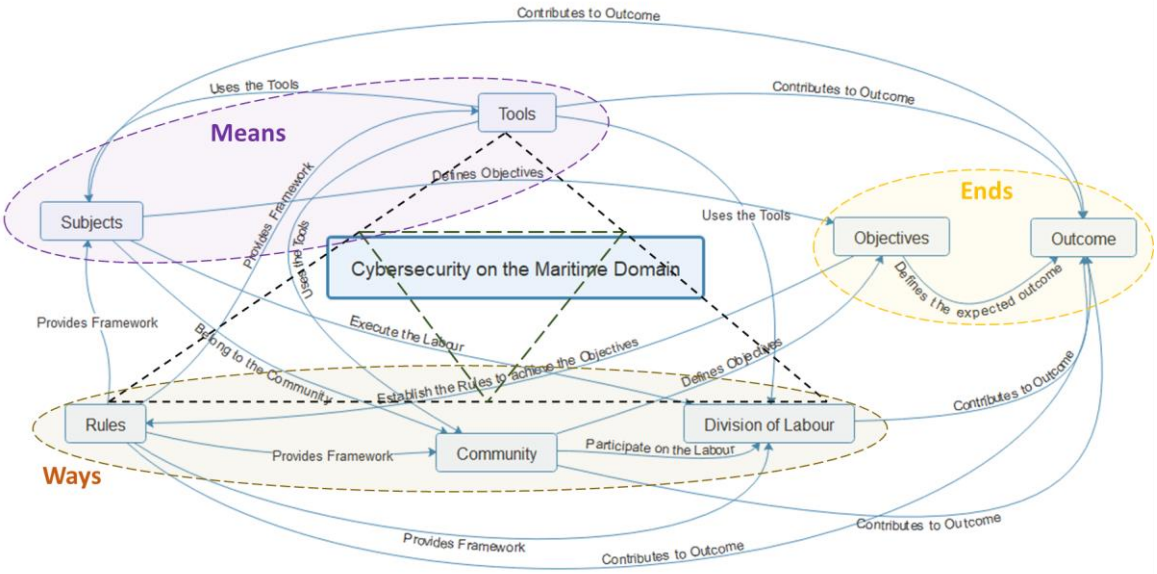


Figure 1-8 - An integrated diagram of Grand Strategy, AT and ANT

If we conduct a generic second-level ANT we must consider the subdivision of each actant in its sub-actants, these new actants will have differentiated roles in the new actant-network, some come from a mediator division, but not all of them are also mediators, some are intermediates, and this must be analysed case by case.

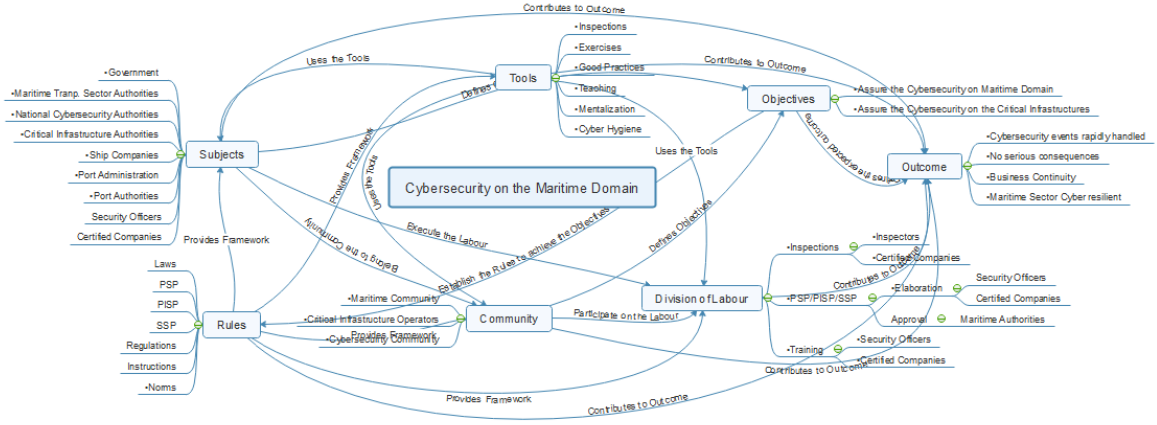


Figure 1-9 - ANT Passing to 2nd Level – 1st Step

When we try to establish the relationships between the actants, we face a complex task, and this only in a generic initial 2nd level approach. Considering the main objective of this work, we felt that, due to its complexity, the ANT approach should be restricted to the analysis of specific relationships or actant-network segments that would contribute to establish the model.

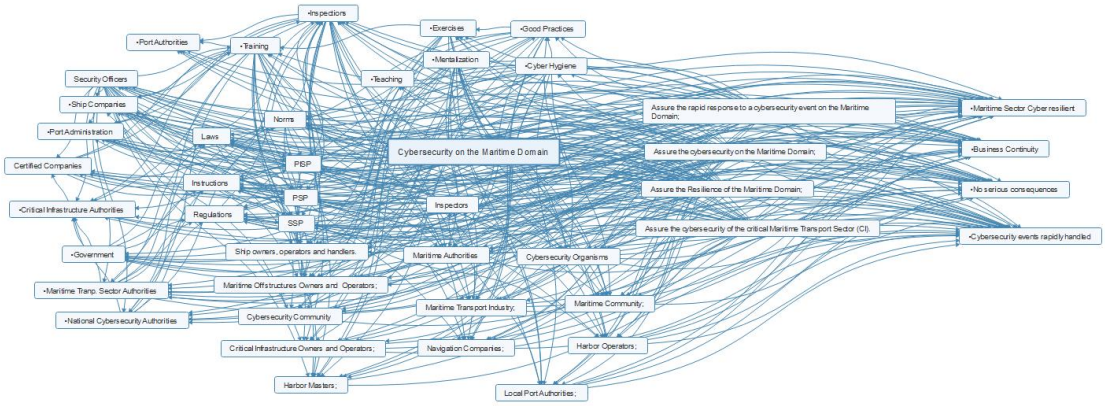


Figure 1-10 - ANT Generic 2nd Level

For this analysis model, we will conduct a 1st Level AT analysis, correlating it with the Grand Strategy, for each target country, in order to obtain the optimal approach and good practices of the observed organisations and afterwards to construct the model applicable to the Portuguese reality. Due to the ANT complexity, we will only conduct a more in-depth level of ANT approach to a specific and more complex actant of the network. A more thorough and detailed ANT analysis should be undertaken in a future work to improve the actant relationship.

1.5. Contributions of the thesis

This thesis has the objective of proposing an organisational model to assure the cybersecurity of the Maritime Domain. Also, this organization will ensure the implementation of the Portuguese Cybersecurity Law (Law 46/2018, of 13 August), that is the transposition of the EU NIS Directive, and verify its compliance.

The organisation proposed must be able to assist the maritime community in the implementation of the necessary measures, procedures and equipment, guaranteeing cybersecurity and conducting security inspections to the ships, port facilities and ports in order to verify the implementation of the approved cybersecurity plans.

To do so, we will choose, through a scientific method, the sample of countries to be studied as a reference and then we will apply the proposed analysis model, explained above, to the information collected, to find similar options and specific choices of each country, the State-of-the-Art Study. Afterwards, we will conduct the same analysis to Portugal, compare it with the findings of the State-of-the-Art Study and built a proposed organisational model to be applied to Portugal.

After the proposed model is built, we will show it to the security experts of the Maritime Community, in the form of a questionnaire, so as to validate it.

In the end, we will present the organisational model liable to ensure cybersecurity on the Maritime Domain that was validated by the security experts of the companies operating in this domain.

1.6. Dissertation Structure

This dissertation is organised into six major chapters. The first chapter explains our motivation to choose this topic, identifies the research question and determines the hypothesis to be answered by this research. Also, it describes the method chosen to conduct the analysis, states what are the expected contributions of this work and describes the structure of the dissertation.

The second chapter is the analysis of the “state of the art” of cybersecurity in the maritime domain of several reference countries.

In the third chapter, we will apply the same analysis to Portugal and compare it with the conclusion drawn from the previous chapter, to help us build the model.

The model proposed is explained in chapter 4 and validated in chapter 5, where we explain the method used and analyse the results.

Finally, in chapter 6 we present the conclusions of this work, envisage the way ahead and propose future works.

2

The “State of the Art”

This chapter explains the “*State of the Art*” of cybersecurity in several reference countries and verifies the existing publications of the area that is issued by those countries, international organisations and maritime security industry.

Due to the limitation in the number of pages, we were obliged to remove from the main volume of the thesis the in-depth analysis carried out to choose the countries, as well as the analysis of the organisation coping with cybersecurity issues in the maritime domain in those countries. This detailed analysis is presented in the Annex “State of the Art” [26] of the thesis that is available along with the main body, the present document.

2.1. General

Cybersecurity presents some unique challenges, including its technical nature, the problem of attribution of the attacks, the fact they can be originated from thousands of miles away and hit without any warning with detrimental consequences in the physical world and logical systems. Possibly most important is that the threat vectors and vulnerabilities changes with every new device, software update, inventive hacker and the strategic goals of the attacker. Therefore, we must recognise that cybersecurity is a process and we should incorporate it into an overall culture of security alongside our physical and human factor security process [27]. The Portuguese National Strategy for Cyberspace 2019-2023 [28] defines cybersecurity as the “*set of measures and prevention actions, monitorization, detection, reaction, analysis and correction that aim to sustain the desired security state and assure the confidentiality, integrity, availability and non-repudiation of the information, networks and information systems in cyberspace, and of the persons that interact on it*” [28].

Harbours, terminals, ships, refineries, and support systems are vital components of all nation’s critical infrastructure, national security, and economy. Cyber-attacks on industrial control systems could kill or injure workers, damage equipment, expose the public and the environment to harmful pollutants, and lead to extensive economic damage [29]. The loss of ship and cargo scheduling systems could substantially slow cargo operations in ports, leading to backups across the transportation system. A less overt cyber-attack could facilitate the smuggling of people, weapons or other contraband [27].

Vessel and facility operators use computers and cyber-dependent technologies for navigation, communications, engineering, cargo, ballast, safety, environmental control, and many other purposes. Emergency systems such as security monitoring, fire detection and alarms increasingly rely on cyber technology [30]. Collectively these technologies enable the MTS (Maritime Transport System) to operate with an impressive record of efficiency and reliability. While these cyber systems create benefits, they also introduce risk. Exploitation, misuse, or simple failure of cyber systems can cause injury or death, harm the marine environment, or disrupt vital trade activity.

Commercial pressure and the ever-increasing demand for speed, efficiency, centralised control, and convenience create incentives to make more meaningful and more integrated use of these systems.

This process increases vulnerability and the "*attack surface*" available to hackers and criminals, as well as to simple misuse. Vessel and facility operators must be able to recognise cyber risks alongside more conventional threats and vulnerabilities. Once recognised, operators should address them via established safety and security regimens, such as security plans, safety management systems, and company policies. [31]

The CIA (Confidentiality, Integrity and Availability) Triad is a familiar, respected model for the development of security policies that are used in identifying problem areas, along with permanent solutions in the arena of information security [32]. These three elements are considered the three most crucial components of security. Also, we must consider a four-element that is the non-repudiation, so we will refer to it has Triad+1.

In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is reliable and precise, availability is a guarantee of reliable access to the information by authorised people and non-repudiation is the assurance that someone cannot deny the validity of something. With more detail, we can describe it as follows:

Table 2-1 – CIA+1 Description [32]

Confidentiality	Integrity	Availability	Non-repudiation
It's crucial in today's world for people to protect their sensitive, private information from unauthorised access. Protecting confidentiality is dependent on being able to define and enforce certain access levels for information. In some cases, doing this involves separating information into various collections that are organised by who needs access to the information and how sensitive that information is - i.e. the	It is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorised party, and it ensures that when an authorised person makes a change that should not have been made the damage can be reversed.	It refers to the actual availability of your data. Authentication mechanisms, access channels and systems all must work correctly for the information they protect and ensure it's available when it is needed. High availability systems are the computing resources that have architectures that are specifically designed to improve availability. Based on the specific HA system design, this may target hardware failures, up-	Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message. Digital signatures (combined with other measures) can offer non-repudiation when it comes to online

Confidentiality	Integrity	Availability	Non-repudiation
amount of damage suffered if the confidentiality was breached. Some of the most common means used to manage confidentiality include access control lists, volume and file encryption, and Unix file permissions.		grades or power outages to help improve availability, or it may manage several network connections to route around various network outages.	transactions, where it is crucial to ensure that a party to a contract or a communication can't deny the authenticity of their signature on a document or sending the communication in the first place. In this context, non-repudiation refers to the ability to ensure that a party to a contract or communication must accept the authenticity of their signature on a document or the sending of a message.

The components of the CIA Triad+1 are equally essential; however, sometimes, we need to give more relevance to one or more than one, depending on the context [32]. According to the situation, one of the aspects can become a priority over others.

The CIA Triad+1 consists of four concepts which represent broad objectives in Information Security. Nevertheless with new types of attacks, like insider, IoT and other threats, new challenges are posed and it is now more difficult to bound and scope these four principles properly [32].

To mitigate the cyber-risks, the nations, in general, take similar steps to identify and prioritise risks, follow the same the process than of other security and safety efforts: assess risk, adopt measures to reduce that risk, determine progress, revise, and continue.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) recommended the development of a cyber-risk management program. The NIST CSF establishes the following functions that are illustrated in Figure 2-1:

- Identify – The administrative structure for cyber risk management as well as the hardware, software, and other components of a system.
- Protect – The technical, administrative, physical, and other procedures to protect systems from failure or exploitation.
- Detect – Procedures to monitor systems and detect when they may have become compromised.
- Respond – The initial actions and notifications needed to limit the consequences of a cyber-event.
- Recover – Follow up steps required to restore full functionality and operations.

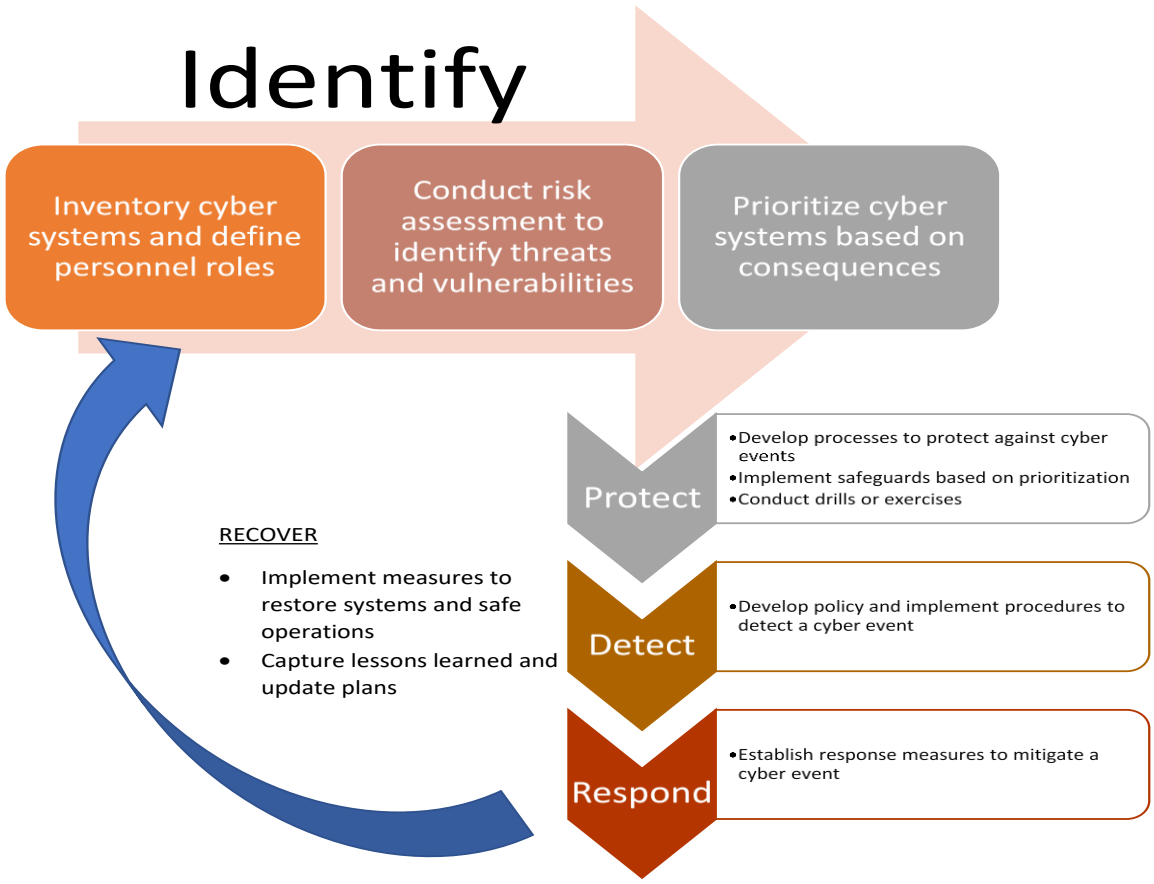


Figure 2-1 - NIST-CSF Functions [33]

The International Maritime Organisation (IMO), in December 2002, introduced changes in the SOLAS Convention (Safety of Life at Sea Convention) that originated the International Code for the Security of Ships and Port Facilities, generally known as “International Ship and Port Facility Security (ISPS) Code”. The EU transposed the ISPS Code into the community law with the European Commission (EC) Regulation 725/2004 [34]. This code has two parts, one obligatory (Part A) and one recommendatory (Part B), but the EU directive made some measures/requirements of Part B also mandatory. [35]

Additionally, there are several IMO documents regarding cybersecurity at sea, such as IMO - Guidelines on Cyber Security Onboard Ships [36] or IMO - Draft Guidelines on Maritime Cyber Risk Management [37]. ENISA also has reference publications on the subject such as the Analysis of Cyber Security Aspects in The Maritime Sector [38] or the Port Cybersecurity - Good practices for cybersecurity in the maritime sector [3].

These are the base of all cybersecurity policies on the maritime domain, as will be shown in the following paragraphs.

2.2. Choosing the Countries to Analyse the Cybersecurity Structure for the Maritime Domain

2.2.1. Basic Criteria

Our selection of the countries to be subjected to our analysis depended on several factors and conditions.

- The countries chosen must accept the MIO SOLAS and ISPS regulations, which allowed a base of security already implemented. This requirement excluded countries that did not ratify these two conventions or did not transpose them to national legislation;
- The nations must have an above-average digital footprint and have defined a national cyber strategy policy. If not, the nations would be in an initial stage of awareness of the dangers of cyberspace. Also, the countries should be above Portugal in the UN e-Government Knowledgebase and the Global Cybersecurity Index, staging, theoretically, in a more mature phase of cyberspace utilisation and, consequently, protection.
- The countries must have implemented a cybersecurity organisation for their cyberspace and have included a specific organisation encompassing the cyberspace of the maritime transport sector. Otherwise, they would not qualify for a study concerning an organisation that they did not possess.

2.2.2. Using the Global Cybersecurity Index and the UN e-Government Knowledgebase as triage.

The first source used for triage was the Global Cybersecurity Index (GCI) [39]. The GCI basis is explained in detail in the Annex “State of the Art”.

On this Index, Portugal scored 0.758 and is the 42nd in the Global Rank, among the High Scoring Countries, but the countries eligible for our analysis should be at a higher level than Portugal. Considering we defined as higher a score of over 0,850, the list of states regarded to be in a Leading Stage (definition adopted from GCI 2017) is reduced to 23.

Leading Stage		
United Kingdom	Canada*	Republic of Korea
United States of America*	Norway	Oman
France	Australia	Qatar
Lithuania	Luxembourg	Georgia
Estonia	Netherlands	Finland
Singapore	Saudi Arabia	Turkey
Spain	Japan	Denmark
Malaysia	Mauritius	

Figure 2-2 - The Nations that Scored Above 0,850

The UN e-Government Development Index (EGDI) is also an important index to sort the nations as to their digital footprint; it is a benchmarking tool that provides a comparative assessment of the e-govern-

ment development of UN Member States. It offers an interactive snapshot of each country's e-government development from a regional and global perspective. (More detailed explanation in the Annex "State of the Art").

Portugal is better classified on this Index, being in the 29th position. In the next step, adopting the same criteria as previously, the countries in inferior rank positions compared to Portugal are automatically excluded, which, in conjunction with CGI, only leaves 14 countries. To further narrow down the number of countries, we applied a social-cultural filter.

Table 2-2 - Comparing CGI and EGDI Index

Country	CGI	EGDI	Country	CGI	EGDI
United Kingdom	1	4	Norway	9	14
United States of America*	2	11	Australia	10	2
France	3	9	Luxembourg	11	18
Estonia	5	16	Netherlands	12	13
Singapore	6	7	Japan	14	10
Spain	7	17	Republic of Korea	15	3
Canada*	9	23	Finland	19	6

2.2.3. The Organisational Culture and Organisational Structures Issue

The solution to apply to Portugal must be easily integrated with the already implemented structure to assure the security of the Maritime Transport Sector, so it must be based on an occidental organisational culture approach, thus excluding the countries that do not share that organisational culture. The detailed analysis and scientific basis are described in the Annex "State of the Art" of this thesis.

Such an assumption is based on several studies which state that organisational culture influences organisational structure [40]. This influence, mainly in multicultural organisations, can lead to new initiatives and good production rates, but requires a disruptive implementation, this always brings resistance to change, and difficulties to implement a non-indigenous culture-based organisational structure [41].

Another aspect is the critical role that culture plays in work motivation and by default in organisational structures. National differences in work motivation are reflected in the legislation, in the decision-making process and by the normal organisational structures adopted. [40]

2.2.4. The Legal Framework

Considering what was previously stated and that after initial research, it was clear that the legal framework constrains the approach to the cybersecurity. The European nations, namely the ones belonging to the EU, share a similar legal framework, resulting in the transposition of the EU regulations and directives to the national laws. This legal framework conditions the organisational structure choices that are made by the countries.

The influence of the legal framework on the organisational structure can also be explained through the Activity Theory (AT). In this theoretical model, we can see the influence of the legal framework on the subjects, on the tool's usage, on the community and consequently on the output of the organisation. Thus, we can state that the legal framework has a crucial role in the organisational structure and outcome.

2.2.5. The Chosen Countries

Regarding the EU countries of the list, it was difficult to find complete information sources on the subject on the Netherlands and Sweden due to the fact that most documents are in the native language.

Under such circumstances, the countries chosen for an in-depth study of their cybersecurity for the Maritime Transport were Spain, France and the United Kingdom. These countries have long ties and an interoperability relationship with Portugal, and there is a mutual influence on the organisational factor due to those ties.

To verify the difference between the reality of EU countries and that of other western civilisation countries and considering that the USA is a reference on cybersecurity issues, an in-depth analysis of the USA organisation for the cybersecurity of the Maritime Transports Sector was also conducted.

2.3. The United States

The primary analysis is done in the Annex “State of the Art” of this thesis, and the results of the application of the analysis model are in Appendix 1 of the main body.

Based on the study, we can state that the USA approach to ensure cybersecurity on the MTS is through the existing organisation of the United States Coast Guard (USCG), the Sector-Specific Agencies (SSA). The USCG adapted its structure to cope with this new reality internally and issued internal doctrine to assure the USCG operations.

The USCG in cooperation with the other organisations. e.g. NIST and with the MTS operators, issued frameworks, regulations and orientations to assure the cybersecurity on the vessels and facilities of the MTS.

To assure the compliance of the MTS actors, vessels and facilities to those requirements, the USCG uses a network of 43 Area Maritime Security Committees (AMSC) in each Captain of the Port zone.

The Captain of the Port (COPT) is responsible for the enforcement, within his respective areas, of port safety and security regulations, including the protection and security of vessels, harbours, and waterfront facilities through inspections, exercises and patrols to the ships and facilities under his Officer in Charge Maritime Inspections (OCMI) role.

Such an organisation can be compared with the Portuguese Maritime Authority Organisation, but it will be necessary to implement the cyber factor on the Portuguese organisation, through doctrine and internal reorganisation.

The promulgation of cybersecurity instructions and procedures to the Portuguese MTS is also required. The inspection system is already in place, but the inspectors are in need of cybersecurity expertise.

2.4. France

The primary analysis is done in the Annex “State of the Art” of the thesis, and the results of the application of the analysis model are in Appendix 1 of the main body.

We can sum up the analysis describing the French approach to assure cybersecurity in the maritime domain as based on the already existing organisation for the implementation and verification of the security of the maritime domain, updating the existing legal framework and adopting the EU and IMO regulations to add the cyber factor to security.

The cybersecurity issue is taken to the highest level of political responsibility, as the prime minister assumes the direct control of the response in a cyber-crisis situation.

To assure the compliance with the regulations, the "*Préfet du Département*" approves the risk evaluation and the security plan for the maritime facilities, and the "*Direction des affaires maritimes*" (DAM) does the same for the French ships. The inspections of the vessels are conducted by the "*Centres de Sécurité des Navires*" (CNS) or certified by the "*Organismes de Sûreté Habilités*" (OSH) and the inspections to maritime facilities are accomplished by the OSH or the agents of the "*Département de la sûreté dans les transports*" (DSûT). Also, the "*Préfet du Département*" is in charge of the response to a security crisis on land and the "*Préfet Maritime*" to a crisis at sea.

Bottom line, the French have a more complex organisation than the United States concerning the implementation and verification of the cybersecurity in the maritime domain, which in the USA is centralised on the USCG but in France is divided by several agents and there are several alternatives of certification and validation according to the law. However, both use previously established organisations to verify the security of the vessels and the facilities.

This type of approach raises the problem of the unity of command when summoned to answer rapidly to an event, a leading body to react to an event must be defined. Sectorial SOCs coordinated by a central Maritime CERT could be the best option.

It is noteworthy that the French organisation in charge of the security in the Maritime Domain is very similar to the one currently implemented in Portugal.

2.5. Spain

The primary analysis is done in the Annex "State of the Art" of the thesis, and the results of the application of the analysis model are in Appendix 1 of the main body.

Concerning the study, we can say very briefly that the Spanish approach to cybersecurity in the maritime domain is identical to the French one. These countries used the existing organisation for the implementation and verification of the security in the maritime domain, updating the current legal framework and adopting the EU and IMO regulations to add the cyber factor to security.

The cybersecurity issue is taken to the highest level of political responsibility, as the prime minister assumes the direct control of the response on a cyber-crisis situation.

The primary coordinator and responsible for the security of the ships is the Maritime Captain. Nevertheless, he is supported in these functions by the General Sub-direction of Security, by the Contamination and the Maritime Inspections Cabinet, and by the harbour protection authority. The Maritime Captain is responsible for assuring the compliance to the maritime protection norms and for approving the evaluation of the port facilities protection, as well as its protection plan. The evaluation of the port facilities protection and its protection plan can also be performed by a recognised organisation of protection.

The State Secretariat for Security resolution of 8 September 2015, which specifies the minimum contents of Security Plans for ships, ports and port facilities, states the need for a holistic approach to security and obliges safety plans to encompass physical security and cybersecurity.

The bottom line is that the Spanish have a more complex organisation than the United States but similar to the French one, with the maritime cybersecurity being divided by several agents and the existence of

several alternatives of certification and validation according to the law. However, the three mentioned countries used previously adopted organisations to verify the security of vessels and facilities.

2.6. The United Kingdom

The primary analysis is done in the Annex “State of the Art” of the thesis, and the results of the application of the analysis model are in Appendix 1 of the main body.

According to this analysis, the UK approach to cybersecurity in the maritime domain is analogous to the other EU nations observed. They all used pre-existing organisations for the implementation and verification of security in the maritime domain, updating the current legal framework and adopting the EU and IMO regulations to add the cyber factor to security.

The cybersecurity issue is taken to the highest level of political responsibility, as the National Security Secretariat (NSC) assumes the direct control of the response in a cyber-crisis situation, as well as in any other crisis.

Furthermore, the UK classifies the cyber-threat at the same level of risk as international terrorism, major accidents or natural hazards, and foreign military crises, making a considerable investment in cyber protection and capabilities.

One specific factor of the UK is that most of the critical infrastructure is owned by privates and it is their responsibility to assure cyber protection under the regimentation framework of the government.

For the maritime domain, the UK issued a specific National Security Strategy and Standards for cybersecurity, and there are two entities that are responsible for the security, both under the Department for Transports (DfT): one for the ships, the Maritime and Coastguard Agency (MCA); others for Ports / Ports Facilities, the Port Security Committee (PSC)/ Port Security Authority (PSA).

According to the UK doctrine, the cyber area must be included in the Ship Security Plan (SSP) and the Port Security Plan (PSP), for which a Cyber Security Assessment (CSA) is developed firstly, being afterwards integrated into the SSP/PSP. On ships, the MCA approves and verifies the compliance of the SSP. In Ports, the Secretary of State of the DfT approves and the Transport Security Inspector of the DfT verifies the implementation of it. A recognised organisation of protection can evaluate the protection of port facilities and their protection plan.

The bottom line is that the organisation of the European countries is similar in very general terms, using previously implemented organisations to assure cybersecurity and imposing cybersecurity measures to be inserted in the security plans of ships and ports.

2.7. Hypothesis answered

So, in this chapter, we have explained the first two hypotheses and partially answered the third one.

The description of the first two hypotheses was done by means of the analysis of the organisation of four different countries, three of them from the EU and the other a non-EU country, the USA. In the study, we could verify the difference between the USA organization and the EU countries and the better adaptability of the models of the EU countries to Portugal rather than that of non-EU nations.

One of the main reasons encountered was the legislation framework, that is common to all EU, due to the fact that EU Directives are mandatorily transposed to national law.

Thus, all legislative framework concerning the safety and security of the maritime transport sector is similar in all EU countries. Also, the implementation of the NIS directive in all EU countries in 2019

homogenised the cybersecurity approach, and so we can conclude that the EU legislative framework is the basis of security and cybersecurity of the maritime domain in the EU.

From the observation of the USA model, we can take valuable lessons and adapt several operational measures on the cybersecurity aspect. Nevertheless, the organizational model itself would be disruptive with the one implemented in Portugal to assure maritime security. If we tried to establish such an organizational model in Portugal, we would face a severe opposition of the organisms included in the Maritime Security System that would not want to lose the power and budget associated with their competences on the maritime security.

Another crucial aspect is the role of the organisational culture and the organisational structure as the main issue to assure a fast adaptation and acceptance of a new organisational structure. We can verify that the organisational structure of the EU Countries differs from the non-European ones.

We also could state that all the countries analysed adapted the existing security and safety organisation for the maritime domain to implement the cybersecurity factor. All of them considered that cybersecurity is one more factor for the safety and security of the maritime transport sector. This lesson was reckoned in the analysis done and was taken into consideration for designing the proposed model.

3

The Portuguese Reality

In the present chapter, we will explain the Portuguese organisation for the safety and security of the maritime domain, discussing the similarities and discrepancies with the other nations that were studied in this work.

Portuguese citizens and industry have good internet access. More than 75% of the Portuguese have internet access, with almost 35% having broadband access. Another interesting fact is that the index of mobile usage exceeds 100% of the population; this mobile usage includes internet access by 3G or 4G. Concerning the 5G, the auction for the frequencies should be held at the beginning of 2020 and telecommunication companies are expected to start commercial usage of the system at the end of next year. [42]

The Portuguese government started the development of e-government in 2006, with the SIMPLEX program. Since then, public services have been digitalised, providing comprehensive public administration services to citizens and businesses through the Internet, so that Portugal has become the 29th country in Europe in e-governance and the 30th in e-participation. [42]

In general, the Portuguese people have an attraction to the digital world, and the amount of e-commerce and e-services is in fast development. Nevertheless, the concerns and awareness about cybersecurity are relatively low and only in 2013 in the *National Strategic Defence Concept* [43] revision, the cyber threats are referred to as one of the new incoming threats. Afterwards, in 2015 the *National Strategy for the Security in Cyberspace* [44] was issued defining the competences of the recently created *National Centre for Cybersecurity* (CNCS) as the nation's coordinator for cybersecurity issues. A new version of the document was promulgated in June 2019.

With the transposition of the NIS directive of the EU (Directive (EU) 2016/1148, of 6 July 2016) [45] to the Portuguese National Law (Law n.º 46/2018, of 13 August) [4], the Portuguese structure for the cybersecurity was clearly defined and the competences and attributions of the CNCS were reinforced.

The CNCS is under the Portuguese Security Authority Cabinet (GNS) and is responsible for assuring the cybersecurity of the Portuguese cyberspace, being the coordinator of all competent authorities in cyberspace. It is also in charge of the cybersecurity of the critical infrastructures, and of the essential service operators and digital service providers. [46]

For these purposes, the CNCS leads the Portuguese Crisis Emergency Response Team (CERT.PT) and is a coordination partner of the Portuguese National CSIRT Network, which includes all the CSIRTS of the major companies, banks and enterprises that operate in the Portuguese Cyberspace.

Only in 2013, the Political Guidance for Cyber Defence [47] was issued, but the National Strategy for Cyber Defence is still under development, its publication being expected for 2020.

In the Minister Council Resolution 92/2019, of 5 June, the second Nacional Strategy for Cyberspace 2019-2023 [28] was promulgated defining 3 strategic objectives with six intervention vectors to orient the development of cybersecurity and cyber-defence capabilities and the fight against digital crime.

Even though Portuguese companies and major enterprises, namely the bank sector, have strong cybersecurity implemented, mainly based on their international experience, most Portuguese citizens, public services and businesses have a shortage of cyber awareness, cyber hygiene and cybersecurity control.

To tackle these issues the CNCS issued two important documents during the current year, the Nacional Reference Framework for Cybersecurity [48], that envisages giving the industries the minimum requisites of cybersecurity they should follow in order to safely conduct their business and the Roadmap to Achieve Cybersecurity Minimum Capabilities [49], which defines a model for the capacitation of the industry on cybersecurity.

Last years, we could see an effort from the government and public associations towards raising awareness and teaching people how to have a safer attitude in what concerns cyberspace.

3.1. Cybersecurity Standards and Legal Framework

To make the legal and organisational framework of the security of the Portuguese flagged vessel and Ports the main document is the Decree-Law 226/2006 of 15 November, that is called the Port Security Law, but also encompasses the security of the vessels.

Portugal has similar law with the other EU countries that were studied in this paper, due to the transposition of the IMO and EU directives concerning the maritime security to the national legislation. These laws are similar but not equal because they vary concerning the national organisation, the nation's interpretation of the treaties and EU directives, so they have some differences that sometimes are significant.

The primary legislation used on the cybersecurity on the maritime domain is the already referred Law Decree 226 / 2006, 15 November; this law decree is a transposition of the SOLAS Convention, the ISPS Code and the EU Regulation 725/2004 of 31 March.

For the cybersecurity in general, Portugal as part of NATO and EU try to transpose those standards to the Portuguese reality.

The transposition of the NIS directive (Directive (EU) 2016/1148 of 6 July 2016) to the Portuguese National Law (Law n. º 46/2018 of 13 August), clearly defined the Portuguese structure for the cybersecurity and the competences and attributions of the various organisms with responsibilities on the cyberspace.

The NIS Directive on security of network and information was the first piece of cybersecurity legislation passed by the European Union (EU). The NIS sets a range of network and information security requirements which apply to operators of essential services (OES) and digital service providers (DSPs). The "*operators of essential services*" referred to in the legislation include enterprises in the energy, transport,

banking, financial market infrastructures, health, drinking water supply and distribution, and digital infrastructure sectors. The NIS Directive requires each EU Member State to put together a list of organisations within those sectors, which they consider to be essential service providers [50].

The specific types of DSPs framework in the Directive include cloud service providers, online marketplaces, and search engines. DSPs should be conscious that the NIS Directive also applies to companies based outside of the EU whose services are accessible within the EU. Moreover, these companies are obliged to assign a EU-based representative to act on their behalf, ensuring NIS Directive compliance. DSPs are, however, subject to a less rigorous framework than the "*operators of essential services*" outlined in the Directive [50].

The NIS Directive includes several requirements around incident response and the implementation of technical security measures based on risk.

3.2. Critical infrastructure and Operators of Essential Services

The entity responsible for the overall protection of the Portuguese infrastructures is the Nacional Council for the Civil Emergency Planning (CNEPC) that in 2003 started a program to identify and issue protection regulations for the critical Infrastructures. [51]

In 2004, Portugal adopted the European Programme for Critical Infrastructure Protection and, in 2008, established the identification procedures and protection norms based on the EU Directive 2008/114/CE. The rules and procedures for European Critical Infrastructures are directly applied to all Portuguese Critical Infrastructures, by the Portuguese Decree-Law n. º 62/2011, of 9 May. [52]

By this decree, the critical infrastructures are divided into two sectors, Energy and Transport, and then separated into eight subsectors, in inland waterways transport and ocean and short-sea shipping and ports are included as specific subsectors.

The critical infrastructure operators are responsible for having an approved security plan for infrastructures, which must be reviewed annually. In that plan, the security of the information systems must be considered. The plan is submitted for comments to the Police, and Civil Protection Authorities and afterwards is sent for approval of the General Secretary of the Internal Security System.

Concerning the cybersecurity of critical infrastructures, the CNCS is the entity responsible for assuring coordination, for issuing norms, for establishing procedures and verifying critical infrastructure operator's compliance. Also, CERT.PT coordinates the national response and helps to liaise with other CSIRTS when the mitigation of the incident must be dealt with foreign entities. CERT.PT actions are done under the subsidiarity principle, meaning that they act as a complement of the action of the entity that has suffered the incident. Subsequently, after the causes of an event have been discovered the CERT.PT will disseminate within the CSIRTs community the conclusions and the mitigation measures liable to assure that this event will not replicate on other operators. [52]

Portugal has identified all OES, as required by the NIS Directive, and has informed the EU about this list and notified all the OES. This has been done along July/August 2019. The NIS Directives require that OES take appropriate technical and organisational measures to secure their network and information systems, account for the latest advances and reflect the potential risks for their systems. Also, they have to take proper steps to prevent and minimise the impact of security incidents, to ensure service

continuity, as well as to inform the relevant controlling authority of any security incident that has a significant impact on service continuity.

The OES must "*without undue delay and, where feasible, no later than 72 hours after having become aware of an incident*" [45] report incidents to the competent authority. The competent authorities will outline incident reporting thresholds for each sector. Presently, these procedures are centralised in the CNCS, but in the future, a coordinating body for each OES sector will be defined. The incident reporting structure has been broken down into two sections [45]:

- Incident response – acts as a support function where the CNCS should be approached for the cyber-related incident; the competent authority or lead government department should be approached for assistance with non-cyber related incidents.
- Incident notification – acts as a regulatory process wherein incidents must be reported to the competent authority, and they will then decide if a follow-up investigation is required.

3.3. Maritime Security / Safety

The Portuguese Maritime Authority System (SAM) is a complex ecosystem, with several entities having jurisdiction, interests, competencies and sometimes overlapping authority.

The SAM has the overall attribution to assure the safety and security of the vessels, ports and port facilities, among others. The SAM is constituted by the Police forces, Customs, Maritime Ports Institute, Port Authorities, Directorate-General of Health, other entities with interest on the maritime domain. [53]

The National Coordination Council (CNN), led by the Defence Minister, assures the coordination of the SAM. It comprises several ministers, the head of the Nacional Maritime Authority (AMN), the heads of the Polices, the head of the Air Force, the Director-General of Fisheries, the General Inspector of the Fisheries, Director General of Health, the President of the Water Institute and the head of the Maritime Ports Institute. [53]

The CNN approves and promulgates guidance for the effective articulation of the entities and organs that execute the state power of the maritime authority.

The AMN is an essential player on the SAM; it coordinates the activities of the Directorate-General of Maritime Authority (DGAM) and the Command of the Maritime Police. The head of the Navy is *ex officio* the head of the AMN for the role of the dual usage of the Portuguese Navy in support of the Nacional Maritime Authority to accomplish its missions. [54]

DGAM principal structures are the Maritime Departments and the Maritimes Captaincies. The maritime area is divided into five Maritime Departments: North, Centre, South, Azores and Madeira, which are commanded by the Maritime Director that coordinates and controls the actions of the Port Captains and is the regional commander of the Maritime Police. Those Departments are divided into Maritimes Captaincies, under the command of the Port Captain.

Figure 3-1 - The Organisation of the General Direction of the Maritime Authority

The Port Captain is responsible, within his jurisdiction area, for the safety and security of the vessels, and has the competence of conducting inspections to verify the compliance of the ships with the law and regulations. He is also the local commander of the Maritime Police. [54]

So, it is under the Port Captain's authority that inspections and documental verification checks of the ships are conducted, one of the documents inspected is the Security Plan of the Ship and the compliance to it is verified.

The Maritime Police (PM) is a criminal police, specialised in subjects of the maritime domain; it is part of the National Maritime Authority for her support to assure the compliance with the law and regimentation within the National Maritime Authority jurisdiction area. [55]

This dual function of the Portuguese Navy on the AMN makes better usage of the Navy assets, mainly to conduct fishing control at sea and to coordinate search and rescue actions. Nevertheless, some legal issues may arise from having a military body controlling and commanding criminal police (PM). A specialist points out that it is unconstitutional to have military under the Ministry of Defence (MoD) controlling police forces under the Internal Security Ministry, since the constitution states that the military cannot interfere in public security unless emergency or war state is declared.

Nevertheless, it is the AMN that has the task of coordinating maritime security in the national maritime spaces and ports, under the coordination of the Competent Authority for the Protection of Maritime Transports and Ports (ACPTMP). This organ is under the Internal Security Ministry and has the criminal police powers specialised in the maritime domain, the PM, also having competence on the safety and security of maritime navigation, the DGAM. [56]

These facts make the AMN a key player in maritime security and an essential asset to the ACPTMP; the role attributed to the Directorate-General for Natural Resources, Safety and Maritime Services (DGRM). [56] The Decree-Law 49-A/2012, of 29 February gives the DGRM competence to promote maritime and port security through regulations, supervision and inspections to organisations, activities, ships, equipment and port facilities by the standing legislation [57].

The ACPTMP has the task to assure protection of the maritime and port sectors, introducing measures of protection to port facilities and the vessels. [58] It verifies the compliance with the Decree-Law 226/2006, of 15 November, which transposes the ISPS Code and the EU Directive 725/2004, 31 March. It also establishes the protection level according to the information received by the Coordination Centre of the Operations for Port Security or by the Security Coordination Centre, the DGAM, for vessels and ports.

The DGRM must check if the vessels and ports, to which the regulations are applicable, have an updated and approved security plan. This state organism is also responsible: for approving Ships Security Plans; to review and approve the security evaluation of ports; and to approve Port Facilities Security Plans, under the advice of the Port Protection Authority.

In articulation with the DGAM, it also approves the Port Security Plan after been sent to the Consultative Committee for the Port Security (CCPP).

Recognised organisations can also perform the risk assessment and the Security Plans of the Ships, Ports Facilities and Ports. The certification of these organisations is done and promulgated by the DGRM.

The DGRM in articulation with the DGAM is the point of contact in what regards assistance to ships and port security.

Concerning ships and ports security, several organisms support DGRM tasks:

- The Port Protection Authority (APP) is responsible for performing risk evaluation and elaborating, maintaining, updating and implementing the Port Security Plan (PSP) approved by the DGRM.
- The Consultative Council for the Protection of Maritime Transport and Ports (CCPTMP) is a DGRM consultative organ, responsible for the coordination of the various entities that intervene in the definition and application of norms, recommendations and proceedings for the protection of ships, port facilities and ports.
- The CCPP has the task of giving suggestions and recommendations to the DGRM concerning the protection of maritime transport, port facilities and ports. It also evaluates the PSP to be approved by the DGRM.
- The Coordination Centre for Port Security Operations (CCOPP), as is shown by its name, coordinates the operations liable to guarantee the security of Ports and is headed by the Port Captain that coordinates the PM, the Port Authorities and other police forces with competences in the port area.

Another entity that has responsibilities on the Maritime transport is the Authority for Mobility and Transports (Autoridade da Mobilidade e dos Transportes – AMT), which has the competence to regulate and inspect the sectors of mobility and inland navigation, railroad and related infrastructure and the economic activities in the commercial and maritime port, as services of general economic interest and network-based activities, through its regulatory, supervisory and sanctioning powers, with powers to protect the rights and interests of consumers and to promote and defend competition in private, public, cooperative and social sectors, in accordance with these statutes and other legal framework. [59] The AMT

has security competence over the maritime transport sector, this competence is exclusively attributed to the DGRM, but, even so, they can comment on the measures taken in the sector.

3.3.1. Port Security

All Ports must be subjected to a risk assessment conducted by the APP, and this evaluation is approved by the DGRM in articulation with the DGAM, after listening to the CCPP.

After this, the APP elaborates a PSP that must be approved by the DGRM, also in articulation with the DGAM, after listening to the CCPP.

The PSP must contain all the PFSP of the facilities within the Port. The PFSP is elaborated by the Port Facilities Administration (AIP), through the Officer of Security of the Port Facility (OPIP), in articulation with the Port Authority.

The DGRM approves the PFSP after listening to the APP.

After the approval of the PSP and the PFSP, the Port undergoes an initial inspection by the DGRM to assure the correct implementation of the security plans. Afterwards, the Port receives a certificate that is valid for five years, and then they undergo a renewal inspection by the DGRM. At any time the DGRM can conduct inspections to Ports in order to assure the compliance with the plans and check if the plans are still adequate to guarantee Port and Port Facilities security or if they must be updated.

The DGRM can also recognise organisations to elaborate the PFSP and the PSP.

3.3.2. Ship Security

Ships risk assessment is an essential part for the elaboration and updating of the SSP, the Company Security Officer (OPC) is in charge of this assessment, and all ships must have a valid risk assessment approved by the OPC.

The OPC is also responsible for elaborating the SSP and presenting it for approval to the DGRM.

All ships must have an International Ship Security Certificate (ISSC), which is requested to the DRGM with a copy of the already approved SSP. For the certificate to be issued, the DRGM has to perform an initial inspection and for the renewal, another inspection will have to take place. At any time, the ships can undergo intermediate inspections to assure compliance with the plans and check if the plans are still adequate to ensure the ship security or if they must be updated.

The AMN assets can perform those inspections, which are usually done by DGAM through the Maritime Captaincies.

3.3.3. Minimum Contents of the SSP, PFSP and PSP

The minimum contents of the security plan are established in the Decree-Law 226/2006, of 15 November, but in these requirements, there is no mention of a mandatory or optional cybersecurity component to the SSP, PFSP or the PSP; the fact that cybersecurity is not considered is alarming.

Several events in recent history show that port facilities and ships are targets for cyber-attacks, generally with criminal intents, but if a terrorist cyber-attack would target an international port this could have cascade consequences in worldwide trade, that is mostly based on maritime transport, as the "*Non-Petya*" event showed.

Also, in October 2013 drug traffickers mounted a sophisticated cyber-attack on the port systems in the port of Antwerp, Belgium. The traffickers employed hackers to intrude into the systems and take control of the movement of containers through the port. It is believed that the initial breach happened in June

2011, and, for over two years, the breach went undetected. Through their access to the system, the criminals were able to hide drugs in containers shipped from South America and then removed the containers from the port before the owner or shipper arrived to collect the container. In other cybersecurity incidents, port assets have been infected with malware, and there has been unintentional jamming or interference with wireless networks. [60]

3.4. Responding to a cybersecurity event

The CERT.PT was a creation of the beginning of the 21st century in the Academic Community. It was transferred to CNCS after its creation in 2014. In 2018, the Law 46/2018 of 13 August gave it clear tasks and competences.

In public policy, the information and communications technology (ICT) infrastructures are typically regarded as critical information infrastructures and, thus, require security and protection against cyber threats. The EU NIS policy combines public and private policies regarding operators, that are highly co-dependent. Any NIS policy success is based on an overwhelming degree of commitment and compliance of ICT infrastructure operators. Increasingly, policymakers must pay attention to the supporting governance system, which would give the best effect to NIS policy objectives. NIS governance objectives can be pursued through public-private partnerships, but not all functions of NIS policy can be suitably achieved at the EU level. [61]

The Cybersecurity Strategy of the European Union clearly asserts the need to establish standard minimum requirements for NIS at national level obliging Member States to designate the competent national authorities for NIS, to set up a well-functioning CERT and to adopt a national NIS strategy and a national NIS cooperation plan. [62] Portugal complies with this directive, at least in what regards legislation and the building of the CERT.

The CERT.PT is in charge of monitoring all events with national impact, disseminating the events and reacting, analysing and mitigating them.

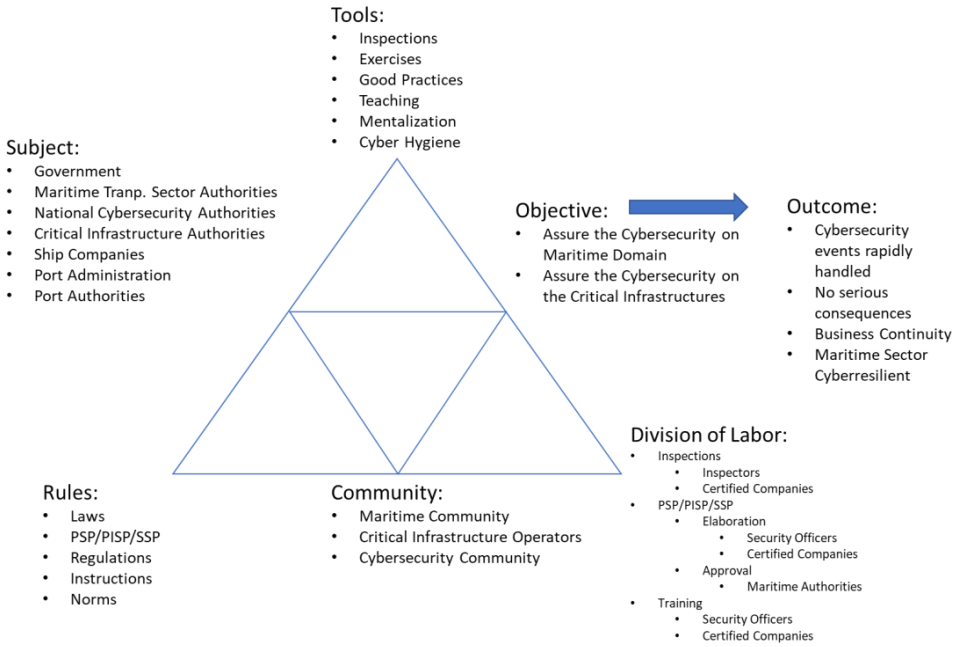
It performs these tasks through the CNCS, creating trust relationships with the public and private sectors with a footprint on Portuguese cyberspace. It tries to establish standard procedures, trust connections between the players and conducts exercises to test the organisation.

For this, the CIRT network was created, the CERT.PT is the coordinator, and the CIRTs of the major companies and public entities share information and events.

Due to the vast number of events in several sectors and the lack of human resources in the CNCS, the CNCS is trying to organise the CIRT network into a network of nodes. The banking institutions have an ISAC (Information Sharing and Analysis Centre) coordinated by the Bank of Portugal CSIRT, which receive all events and share the information between the several banks CSIRTs, keeping informed the CNCS and, if necessary, requesting its technical support. These facts allow the sector to share in confidence cyber events with a common purpose and wording specific to one sector.

With this view, the organisation proposed to cope with cybersecurity in the Portuguese maritime domain will include a Maritime ISAC.

3.5. Activity Theory Analysis



To conduct the analysis of the country profile in cybersecurity in the maritime domain, we will present a scheme of the Activity Theory.

Objective Why is the activity taking place?	Outcome: What is the desired Outcome from carrying out this activity?	Subjects: Who is involved in carrying out this activity?	Tools: By what means are the subjects performing this activity?
Assure cybersecurity in the Maritime Domain; Assure the Resilience of the Maritime Domain; Ensure a rapid response to a cybersecurity event on the Maritime Domain; Simultaneously, assure cybersecurity of the critical Maritime Transport Sector (CI).	The Maritime Domain is Cyber resilient; The Maritime Domain Community has cyber hygiene knowledge and behaviours; All cyber events in the Maritime Domain are rapidly dealt with and analysed; Lessons are learned from the events and result in new best practices or norms; The Maritime Domain actors have SSP / FSP implemented and validated; C4All Maritime Domain actors know their role in the maritime cybersecurity organisation; The Maritime Transport Critical Sectors are cyber protected.	Prime Minister Defence Minister National Centre for Cybersecurity (CNCS) Portuguese National CSIRT Network National Council for the Civil Emergency Planning (CNPCE) Portuguese Maritime Authority System (SAM) National Coordination Council (CNN) Nacional Maritime Authority (AMN) General Direction of the Maritime Authority (DGAM) Maritime Departments Maritime Director Port Captain Maritimes Captaincies Competent Authority for the Protection of the Maritime Transports and Ports (ACPTMP) General Direction of the Natural Resources, Safety and Maritime Services (DGRM) Consultative Committee for the Port Security (CCPP) Port Protection Authority (APP) Consultative Council to the Protection of the Maritime Transport and Ports (CCPTMP) Recognised security organisations Company Security Officer (OPC) Authority for the Mobility and the Transports (AMT)	Mandatory Formation for Key Roles Mandatory cyber hygiene formation Mandatory schedule of exercises Inspections Cybersecurity Information Sharing; Incorporate Cybersecurity into Training and Education; CERTs CSIRTs SOCs

Rules: Are there any cultural norms, rules or regulations governing the performance of this activity?	Community: What is the environment in which this activity is carried out?	Division of Labour: Who is responsible for what, when carrying out this activity and how are the roles organised?
EU Directive 2008/114/CE - Critical Infrastructures EU Regulation EU Regulation n. º 725/2004 - transposition of the SOLAS Convention, the ISPS Code EU Directive 2005/65/EU - Enhancing port-security IMO MSC-FAL.1-Circ.3 - Guidelines on Maritime Cyber Risk Management MSC—96/WP.9 - Measures to Enhance Maritime Security FAL 40/INF.4 - Guidelines on the Facilitation Aspects of Protecting the Maritime Transport Network from Cyber threats ISPS (International Ship and Port Facility Security) (IMO 1998) SOLAS convention (IMO 1974) Law-Decree n. º 62/2011, 9 May transposition of EU Directive 2008/114/CE Ship Security Plan (SSP) Ship Security Assessment (SSA) Port Facility Security Plan (PFSP) Port Security Plan (PSP) Port Facility Security Assessment (PFSA) Port Security Assessment (PSA) Cyber Security Assessment (CSA) Law Decree 226/2006, 15 November - transposition of EU Regulation 725 / 2004 Directive (EU) 2016/1148, 6 July 2016 - NIS directive Law 46/2018, 13 August - transposition of Directive (EU) 2016/1148 Nacional Reference Framework for Cybersecurity Roadmap to Achieve the Cybersecurity Minimum Capabilities Minister Council Resolution 92/2019, 5 of June - Nacional Strategy for Cyberspace 2019-2023	Maritime Transport Industry Harbour Masters Navigation Companies Harbour Operators Maritime Community Critical Infrastructure Owners and Operators Maritime Off structures Owners and Operators Local Port Authorities; Ship-owners, operators and handlers Maritime Authorities Cybersecurity Community Cybersecurity Organisms	Prime Minister - Leads the Council of Cyberspace Council Defence Minister - Leads the CNN CNCS - Centralizes all cybersecurity events response, including the maritime Portuguese National CSIRT Network - Information sharing CNPCE - responsible for the overall protection of the Portuguese infrastructures SAM - ensures the safety and security of vessels, ports and port facilities CNN - approves and promulgates guidance for the effective articulation of the entities and organs that execute the state power of the maritime authority AMN • coordinates the activities General Direction of the Maritime Authority (DGAM) and the of the Command of the Maritime Police • assure the maritime security in the national maritime spaces and ports Maritime Director - coordinates and controls the actions of Port Captains and is the regional commander of the Maritime Police Port Captain - is in charge of the safety and security of vessels, and conducts inspections to the ship DGRM • together with ACPTMP, has the task to ensure the protection of maritime and port sectors, introducing measures of protection to port facilities and vessels • approves the SSP, PFSA, PFSP, PSA and the PSP • conducts port inspections CCPP - gives his opinion concerning the PSP APP - conducts the PSA and implements the PSP approved CCPTMP - coordinates the various entities that intervene in the definition and application of the norms, recommendations and procedures for the protection of ships, port facilities and ports. Recognised security organisations - can conduct port and ship inspections OPC - conducts the SSA and SSP and submits for approval. Afterwards, implements it.

3.6. Other Variable Analysis

CGI Rank	**42**
E-Government Rank	29
Is maritime transport a CI?	Yes, the CI is divided into two sectors and eight subsectors, Transport is a sector, and transports in inner waters, maritime transports and ports are subsectors.
Specific Cybersecurity Organism?	National Centre for Cybersecurity (CNCS)
Specific Cybersecurity Organism for Maritime Domain?	No, there is no clear definition of who is responsible for cybersecurity in the maritime domain.

Specific Rules / Law for Cybersecurity in the MD?	No
The Security Laws were adopted to Include Cybersecurity in the MD?	No
Was a new organisation adopted to cope with cybersecurity in MD?	No
The PSP, PFSO and PSP encompass cybersecurity?	No
Is there a specific Organisation to respond to a Cybersecurity event in the MD?	Yes, there is. In general terms, for all the cybersecurity events the response is through the CNCS and the CERTs. Nevertheless, nothing is mentioned concerning the reaction to a cyber-event, specifically, in the maritime domain.

3.7. The Grand Strategy Interpretation of the Results

Considering the board that was presented in Table 1-3, we can say that all countries observed have the same Ends concerning cybersecurity in the Maritime domain. All the states want to ensure cyber protection of the Maritime Transport Critical Sector guaranteeing its resilience and business continuity. It is crucial to the economy of the country that the Maritime Transport Sector is secure. A significant event on a commercial harbour can give rise to cascade consequences and it may have an impact on the national and regional economy. It is so because maritime transport is essential to the global economy: over 90% of the world's trade is done by sea, and it is, by far, the most cost-effective way to move mass goods and resources across the globe. [63]

Also, cyber-attacks to shipping companies can have a significant impact on countries and world economy, as was shown by the "NonPetya" event that caused accumulated losses for Maersk Line, more than $350 million according to Adam Banks, chief technology and information officer at Maersk. [64]

Concerning the ways to achieve that end, even if we have the same environment, in broad terms, we may follow two different approaches, one from the USA and the other from the EU. As was previously explained, the USA approach is more centralised in the USCG with the contribution of the private sector and NIST; in Europe we have several entities with tasks on the sector, working, basically, with the same legislative framework and using the same tools to achieve that goal. Even with a coordination body, that most of the times is on the strategic level, it is a more complicated and protracted task.

These facts also imply a more decentralised way to conduct the tasks and the need of a more detailed and spread division of labour, with the consequent necessity of more coordination boards and committees, to achieve the ends.

Consequently, the means to attain those goals will vary according to the subject's actions and the necessary tools. Even if the tools are similar in all the countries, the variety of subjects leads to the need for multiple resources to accomplish the task. The higher number of intervenients and organisations will necessarily imply more resources to meet the ends and a greater need for coordination to optimise the

resources used and avoid unnecessary duplication. So, we can affirm that the USA approach requires significantly fewer resources and means to implement and ensure cybersecurity in the maritime domain than the European approach.

Considering the logic of the:

Suitability (Does the achievement of the objectives give us the strategic effects that we seek for?). If we can achieve the ends that we proposed for, we will accomplish the strategic effects that we seek, and we will have a critical sector cyber protected, resilient with a business continuity assured that allow us to minimize the damaged of a cyber event of our maritime domain in our economy and society.

Acceptability (Do those strategic effects justify the targeted objectives and the methods and resources necessary to achieve them?) Considering the devastating effects that an uncontrolled event could have in our society and economy, local and worldwide, the resources needed to implement the ways to achieve our ends are considerably low when compared to the resources required to achieve lower strategic objectives. This activity depends widely on the functional organization implemented, the coordination procedures, and leadership. It also relies on human resources, formation and good practices and, on a minor scale, on the usage of the correct hardware and software.

Feasibility (Are the strategic concepts achievable with the available resources?) This is a matter of priorities but, as has already been mentioned, the resources needed are considerably lower than the needs for other strategic objectives, the human factor being the critical resource.

Considering the above analysis, we can conclude that Portugal has adequately defined the ends, in parity with the other EU countries observed, namely in terms of the Strategy for the Cyberspace Security 2019-2023 and the National Reference Framework for Cybersecurity, but concerning the ways and the means, it must improve in order to achieve the proposed ends.

Namely, it should be included in the legislative framework that the SSP, PFSP and PSP must encompass cybersecurity measures and the creation of the CySO functions. Also, it must create an organisation with the capacity to conduct inspections concerning cybersecurity on the ships and harbours, and it is necessary to establish a coordination and information dissemination centre for the maritime domain, defining a coordinating entity for the cyber aspect in the maritime domain, among others.

3.8. Comparing the Analysis Results of the Activity Theory

When we compare the analysis based on the theoretical model of the Activity Theory applied to the chosen countries, we observe several interesting facts and reach some conclusions.

As expected, since the four chosen countries are “western societies”, we notice that three of the observed fields are similar, almost equal in all of them: The Objective, the Outcome and the Community. The four countries have the same objective for the establishment of this organisation, they expect the same results and they have similar environments in which this activity is carried out.

Another relevant fact is that the USA has one entity that is the crucial player for cybersecurity in the Maritime Domain — the USCG —, and the European countries have a multiplicity of organisms, committees and organisations, belonging all to the state, that have competences and jurisdiction in the Maritime Domain, at least in a small fraction of it; this can cause a problem of command unity to respond to an event and raises the need to have a centralized reaction organism with necessary competencies in

the maritime domain. This also confirms our premise that the USA differs substantially from the European countries concerning the organisational structure. As a result, the division of labour reflects the complexity of the organisational structure of the Europeans countries, with several different organisms and entities assuming various tasks. Even when there is a coordination organism of the board for the task, routine activities can be difficult to coordinate and synchronise, with frequent overlapping of functions and power struggles about who has jurisdiction on what. So, as previously mentioned, there is a need of an organism to ensure the unity of command in the reaction to a cybernetic event in the maritime domain, otherwise, the reaction could be considerably delayed, which can have severe consequences. Nevertheless, to implement a new organisation in the required timeframe, it is mandatory to implement the existing structure. A disruptive organisation would take longer, consume more resources, originate the opposition and resistance of the current organisms, unwilling to let go of their competences or even to share the domain with an outside new organisation. For that reason, the approach similar to the USA for Portugal would be disruptive, even if we can take very good lessons on the operational procedures from the USCG concerning the cybersecurity issue. Thus, as we are looking for a smooth first approach to the subject that would be easily accepted by all the actors, we will not apply this approach in the proposed model.

We also can notice that all the countries have a similar approach to how the subjects perform the activity; this means that they use similar tools. This approach is based on reaction plans, inspections, formation plans for specific roles, cyber hygiene tutorials for all elements, information sharing, and security and reaction centres.

Concerning the Rules, the main factor that we can observe is the legislative framework. Here we can confirm, again, the difference between the USA and the European countries observed. One of our premises was that the legal framework would influence the organisational structure adopted and, due to this, we chose European countries that belong to the EU, so all the states would have EU Directives and regimentation as the basis complementing the SOLAS Convention and ISPS Code from IMO. Even if the USA framework considers the SOLAS and ISPS Code, it also has several norms and regulations of other sources, as NIST and other inputs, mainly from the private sector, which differs from the EU approach in the broad terms. Meanwhile, all the European countries base their legislative framework on EU Directive 2008/114/CE (Critical Infrastructures EU Regulation), EU Regulation n.º 725/2004 (transposition of the SOLAS Convention, the ISPS Code), EU Directive 2005/65/EU (that enhances port security) and Directive (EU) 2016/1148 of 6 July 2016 (the NIS directive).

Comparing the other European Countries with Portugal we notice that Portugal has a similar organisation to cope with security in the Maritime Domain, and it shares the same objectives, expected outcomes, tools, community and legislative frameworks (having transposed to national legislation all the EU Directives and Regulations). Nevertheless, it still has to impose cybersecurity through these norms, lacking specific instructions to encompass cybersecurity in SSP, PFSP and PSP. Also, we are in need of an organisation to disseminate and coordinate cyber events in the Maritime Domain.

3.9. Inferences

In conclusion, Portuguese reality has specific regulations concerning cybersecurity in general, but lacks a doctrine concerning the maritime sector. Portuguese maritime domain is too complex and important to be able to reach its objectives only with doctrine. These regulations must be adapted specifically for the maritime cybersecurity, only then will it be possible to have an effective and operational doctrine and policy for the sector, based on the national and EU policy framework. Without this, it is not possible to implement that framework on the Portuguese Maritime Domain.

Portuguese adhere widely to new technologies, but lack cyber hygiene habits and, most of the times, they are unaware of the dangers of cyberspace.

The Portuguese Government and several other organisms are beginning to understand the need to have a safe cyberspace, assuring a secure growth in the usage of Portuguese cyberspace. With that purpose, the government has started to launch and implement several measures to urge individuals as well as businesses to have safer behaviours and to implement the correct safety controls that will result in a more secure cyberspace.

The transposition of the SOLAS Convention and the ISPS Code to national law was accomplished, based on the EU directives and regulations (that made mandatory parts of the ISPS which, in the code, were only recommendations). The Portuguese interpretation differs from the UK's concerning the inclusion of the cyber factor in the SSP. The UK considers that it is mandatory in the European legislation and in the ISPS Code, through paragraphs 8.1 to 8.10 of Part B of the ISPS Code, which provides guidance on aspects to be included in the SSA, like radio and telecommunication systems (including computer systems and networks); the Portuguese law does not transpose that interpretation.

Portuguese and French organisations are very similar, but France has clearly defined the inclusion of the cybersecurity factor in the SSP, in the PFSP and in the PSP, and Portugal has not.

The significant advantage of the USA organisation, compared to the European countries analysed in this work, is that the USA has integrated all services into a single organisation. The USCG has all the authority defining the contents, approving and then inspecting the security plans of the maritime sector; this only requires internal coordination and a hierarchical superior that can determine the priorities and resolve any conflict.

In the other countries, particularly in Portugal, the various entities are most of the times under different Ministers, with different interests, which makes the coordination between them more difficult, even having a designated coordination mechanism. More complicated issues require coordination boards presided by the Prime Minister to meet, and this procedure delays the main decisions and creates conflicts between the entities responsible for cyberspace in the maritime domain.

In short, Portugal has an organisation generally similar to that of the other analysed European countries but is still behind concerning the implementation of control measures and regulations to assure the cybersecurity of the maritime domain. Any organisation to implement these controls and issue the necessary rules, regulations and proceedings must be conceived using the already implemented security organisation in close coordination with the CNCS.

The inferences in this section support the validation of the third hypothesis.

4

Proposed Model

Given the previous chapters, this one introduces the model proposed to face the Portuguese reality on cybersecurity in the maritime domain.

The Portuguese organisation for ensuring maritime domain security bears general similarities to that of the other EU countries, with the responsibility being scattered throughout several state organisms.

The maritime transports and ports are considered a critical sector in Portugal, and it has already specific legislation concerning critical infrastructure, as explained previously, which includes the information systems and the need to protect them. Also, specifically for the transport sector, the transposition of the EU NIS directive to Portuguese Legislation points out the need to ensure cybersecurity in the sector of transport and in the subsector of maritime transport, including inner waters maritime transport, specifying maritime transport companies, Port Authorities and Maritime Transport Operators.

How the implementation of the NIS directive in the Portuguese Maritime Sector will be assured is still an empty spot, with the clear notion that the CNCS does not have the capacity, for lack of human resources and expertise required in this sector. That will demand synergies between the sector operators, namely an entity responsible for coordinating the security of the sector and the CNCS.

As already mentioned, the Portuguese organisation for the safety and security of Maritime Ports and Transports comprises multiple entities with responsibilities in this area, and they have occasional overlapping competencies. The action of these authorities is coordinated by the DGRM, that uses the AMN as the coordinator in security aspects.

However, due to the variety of the participating organisms on the SAM, often it becomes impossible for the DGRM to coordinate their actions without having to appeal to the National Coordination Council, presided by the Defence Ministry. This fact always makes one of the organisms to feel impaired by the other party and refrains the application of a certain measure or decision.

This problem often arises in the context of maritime security, and several issues still lack an explicit controlling entity. Sometimes doubts concerning the authority in a specific subject create conflicts between the various organisms that claim to have the competence to resolve such issues.

Another controversy in the security of the Maritime Domain is the nonacceptance by other organisms of the criminal police competences of the AMN through the Maritime Police (PM); they state that the AMN

is a military enclave in a public domain of security. Due to the dual role of the Portuguese Navy, the head of the Navy is the head of the AMN, and Port Captains are Navy Officers. These facts generate strong opposition from the civilian organisms, that envisage an opportunity to gain competences, power and increase their budget, while reducing the role of the Navy in the security of the Maritime Domain. We can find references to these facts in the Portuguese media, e.g. [65].

The Decree-Law 49-A/2012, of 29 February, clearly establishes the DGRM as the entity competent to promote maritime and port security. The DGRM determines regulations, supervises and conducts inspections to the organisations, activities, ships, equipment and port facilities according to international and national rules. The Decree-Law 226/2006, of 15 November, states that the AMN is the entity that supports DGRM in the coordination of all those intervening in the security of maritime spaces and ports. The AMN has a police body with criminal police competences, specialised in the maritime domain and competent to ensure the safety of navigation.

Concerning the cybersecurity issue in the maritime domain, it is necessary to implement a new organisation, norms, regulations and proceedings that may verify the compliance with the NIS directive on maritime transports and ports. This organisation must be drawn using the one already established in close coordination with the CNCS.

Considering the results of the analysis of the chosen countries' models, we must define a model based on the actual security organisation for the Maritime Transport Sector considering the existence of a specialised entity to coordinate the cybersecurity aspect of the sector. Also, it is necessary to conduct an adaptation of the legislative framework, or at least, to implement proceedings, norms and regulations that define the minimum cybersecurity standards in the Maritime Domain, complying to the demands of the NIS directive.

The implementation of cybersecurity standards in the Maritime Transport Sector must always be a teamwork of all SAM and all the operators of the domain. Without the participation and collaboration of all, this implementation will never be successful.

4.1. Proceedings, norms and regulations

Proceedings, norms, regulations and good practice guides can be easily found in official and trusted sources. Therefore, it is not necessary to start the process to produce such documents from scratch; we only need to analyse the existing ones and adapt to the Portuguese reality the ones that we think are the best suitable or more adapted to Portuguese reality.

This work must be done by the Maritime Domain specialist in cooperation with the CNCS, always in coordination with DGRM. These entities must couple with the task of ensuring cybersecurity in the Maritime Domain, ideally with a legislative revision providing the needed legal framework support.

One of the best and more straightforward norms and proceedings to apply in a short time with a robust structure is the IET Standards for Cybersecurity for Ships [34] and the IET Standards for Cybersecurity for Ports and Port Facilities [60]. These two documents are very well structured, they are simple to apply and have a sound legal basis on the SOLAS Convention, ISPS Code and EU regulations.

These two standards clearly define the process from risk assessment to the elaboration of the Ship / Port Facility / Port Cybersecurity Plan, to their integration as annexes of the SSP, PFSP and PSP. It

also structures the cybersecurity organisation of the ship/port to assure the training, the upkeep of the standards and protocols, and the update of the Cybersecurity Plans.

These documents define key personnel that must have specific education and must be certified by an education entity recognised by the governmental organism responsible for cybersecurity in the maritime domain. If we were to transpose this to the Portuguese case, the body to recognise the certification centres should be DGRM or other government entity designated by it.

Other publications issued by other countries are complete and present similar organisations coping with the cybersecurity management in the maritime domain, namely the USA, but even if they very comprehensive, they are not as straight forward to apply as the UK's IET or the IMO guidelines [36].

Portugal has a gap in this field, which should be filled with the application of regulations that are simple and easy to implement without considerable expenses to the operators. All players must be aware that the lack of investment in this area will demand, in the near future, substantial investment in technologic infrastructure to reach the minimum standards liable to ensure the cybersecurity of the systems. Also, the education of the specialised personnel, responsible for implementing and monitoring the controls and IT, and the general cyber hygiene of all employees can have considerable costs.

The update of older SCADA equipment present in many port facilities and ships and the inboard networks can also demand a considerable investment in new equipment, and in logical and hardware upgrades.

Due to this fact, the level of demand must be gradual giving the operators time to adopt and conduct reasonable investments with state support, at least at the technical level. Afterwards, the regulations can be made more complete and complex with measures that were first advisory afterwards becoming mandatory.

4.2. Public-Private Partnership (PPP)

The EP3R (European Public-Private Partnership for Resilience) was established in 2009 and was the very first attempt at Pan-European level to use a Public-Private Partnership (PPP) to address cross border Security and Resilience concerns in the Telecom Sector. The large number of PPP experiences worldwide has confirmed the value of such approach also for its flexibility and appropriateness for today emerging challenges including cyber-attacks mitigation, critical infrastructure protection and security and resilience of information and communications. [66]

PPPs are, in policy as well as in academic circles, often considered a model of organisation that can enhance flexibility and robustness by including a broader range of civil and private actors. In partnership meetings, private businesses are called upon to share knowledge on national security voluntarily and to assume responsibility for ensuring effective management of cyber threats. Despite a firm agreement about the characterisation of cyber-security risk as a 'shared risk', the turn to partnerships does not itself establish what kind of knowledge the different partners should share. Instead, the fundamental uncertainty associated with cybersecurity seems to have opened the space for contestation over 'what to counter', and thus what counts as cyber-security knowledge.

PPPs entail an inherent tension between the functional differentiation of the public and private sectors, on the one hand, and the unity conferred by a 'sense of community' and loyalty on the other.

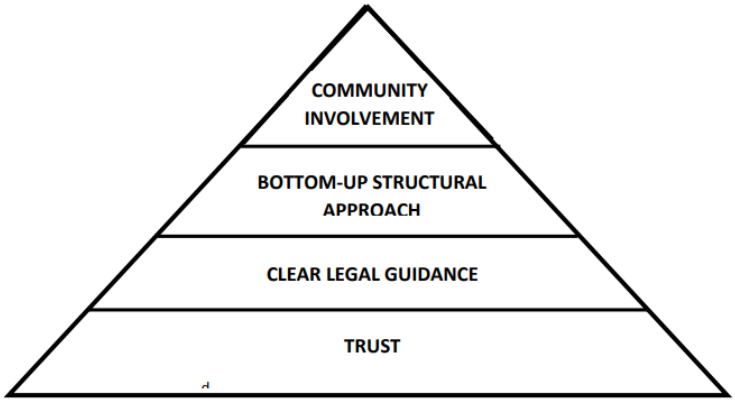


Figure 4-1 - Qualitative Model for Successful Public-Private Partnerships [67]

The first step to any successful PPP is for all parties to agree and build a high level of trust. Nearly every piece of literature studied covering PPPs mentioned the significance of trust within the commitment.

While the first level of the model regards building a sense of trust among the parties within a PPP, the next step focuses on establishing clear baseline legal guidance to nurture a trusted relationship. PPPs can be formed in two different ways, which are collaborative (non-legally binding) or contractual (legally binding) agreements.

For when applying clear legal guidance, the next layer in the model for a capable PPP is establishing a bottom-up approach for the organisational structure of the PPP. For example, Australia and Great Britain have in place strict “draconian measures” in their PPPs with private companies for how those companies are to invest in cyber defence and share internal data about attacks. The level of sharing is reportedly limited due to the established top-down approach to the relationship. On the other hand, there is a successful example of a cybersecurity PPP in the Netherlands. In the Dutch collaboration, the National Cybersecurity Centre (NCSC-NL) actively encourages participation from the private companies via conferences held where public and private organisations physically sit down together and discuss all the terms and conditions for how the network sharing is constructed. Also, the CNCS uses this model, normally flameworked by a protocol, to mainly address the education and sensibilisation areas.

The final level, the highest point of the model, is the influence of the community involved, both within the organisations and outside, in rallying support for the parties to enter a PPP. [67]

Strategic EU documents on cybersecurity repeatedly emphasise the role of PPPs and private-sector collaboration in combating cyber-attacks and cybercrime. This tendency to view PPPs as the organisational answer to the management of new threats to national security has been particularly active in the United States, where the number of PPPs on security has increased significantly: we have counted more than 100 security partnerships involving either the Department for Homeland Security or the FBI. In Europe, the scale of this kind of public-private collaboration is smaller, and we have yet to see the same type of institutionalisation. However, despite the national differences, western private companies are increasingly considered relevant to the security of the nation. [68]

Promotion of collaboration between public authorities and private companies (mainly critical infrastructure companies) has been central to efforts to manage the rising challenge of cybersecurity. [68] Also, the Portuguese Nacional Strategy for Cyberspace 2019-2023 is the sixth intervention vector encompassing this subject.

EU offers a rather elaborate discussion about the specifics of the desired cooperation of public authorities and the private sector. Specifically, it suggests that the role of the former is to ensure "*free and safe cyberspace*", which translates in the following tasks: "*to safeguard access and openness, to respect and protect fundamental rights online and to maintain the reliability and interoperability of the Internet*." For private sector actors, the strategy claims that they "*should continue to play a leading role in the construction and day-to-day management of the Internet*," but it also stresses that "*the need for requirements for transparency, accountability and security is becoming more and more prominent*." Thus, it calls on the private sector to identify causes of cyber incidents and conduct forensic investigations; develop, at a technical level, its cyber resilience capacities; and share best practices across sectors, including the public sector. [69]

In 2004, the European Network and Information Security Agency (ENISA) was established and aimed to become a European 'hub' for exchange of information, best practices and knowledge in the field of Information Security. For that, is the main effort is to the establishment of PPPs, which it considers to be essential for the Security and Resilience of Critical Information Infrastructures (CII).

The findings of a recent study of the role of private financial institutions in the fight against terrorist financing suggest that PPPs are not always producing the expected win-win solutions, either for the public or the private sector due to [69]:

1) disagreements about the definition, scope and methods of analysis of the threat of terrorism to individual private financial institutions;
2) information sharing complications arising from the legal impediments to sharing classified information between public agencies and private companies, as well as the persisting lack of trust among many of their representatives;
3) the dissonance between the "better safe than sorry" logic of public security agencies and the "profit first" logic of private companies.

To address these challenges, the EU Cybersecurity Strategy suggested the need to adopt new EU legislation. This legal document must aim to ensure that private businesses in a number of critical areas (energy, transport, banking, stock exchanges, and Contributions of enablers of essential Internet services) assess the cybersecurity risks they face, ensure the reliability and resilience of networks and information systems via appropriate risk management, and share the required information with the national NIS authorities.

With this purpose, the NIS directive (Directive (EU) 2016/1148 of 6 July 2016) applies to two types of operators: Essential Service Operators and Digital Services Providers and requires that the essential service operator uses technical and organisational measures to manage and minimise risks and react to events. The essential service operators must conduct security assessments, mitigate the risk, implement security measures imposed by the regulators and comply with the mandatory notification of incidents. The noncompliance with this directive will have consequences to the essential operators.

Among the key actors of the PPPs are the Information Sharing and Analysis Centres (ISACs), also widely supported by the CNCS that issued specific instructions to help the edification of this type of organisms. These non-profit organisations provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure). Also, they allow two-way sharing of information between

the private and the public sector about root causes, incidents and threats, as well as sharing experience, knowledge and analysis. [70]

European legislation like the NIS Directive and the Cybersecurity Act nourish the creation of sectoral ISACs and PPPs within the EU. The NIS Directive, among others, splits the operators of essential services into sectors and tasks the operators to implement requirements on incident reporting. The creation of sectorial ISACs at the national level could further assist with the implementation of these provisions. Information sharing between national stakeholders but even in cross country cases is a critical aspect of cybersecurity. Knowledge on tackling cyber-attacked, incident response, mitigation measures and preparatory controls can be shared between the relevant stakeholders.

European ISACs are concentrated on creating partnerships and building trust bonds between the members. They are primarily industry-driven, but governmental support is expected because it gives the ISAC an increased formality and corroborates the public sector's respect of industry needs and supports it in facing new challenges

To ensure the right level of cybersecurity, the collaboration between the public and the private sector is crucial. ISACs create a platform for such support in terms of sharing information about root causes, incidents and threats, as well as sharing experience, knowledge and analysis. [70]

For these reasons, it is crucial the establishment of an ISAC for the maritime domain that encompasses all the actors that play on the Maritime Transport Sector, a vital sector for Portugal by the established law.

After the ISAC implementation, with all procedures and regulations inplace, the establishment of a Sectorial CERT should be considered, as we can see in the banking sector.

4.3. The role of the ISAC

After the promulgation of the legal framework for the Portuguese cybersecurity (Law 46/18, of 13 August) and the new National Cybersecurity Strategy 2.0 (2019) of Portugal, the CNCS wants to develop and implement sectorial and geographic ISAC to assure the security of the Portuguese cyberspace.

The relevant roles that ENISA foresaw for this organism and the success of a similar organisation in the USA and UK have already been referred. Due to this fact, the ISAC is seen as a masterpiece to assure the NIS implementation of the EU.

As was explained before in the PPP section, it is crucial to ensure the right level of cybersecurity, cooperation between the public and private sector. The ISACs create a platform for such collaboration in terms of sharing information about root causes, incidents and threats, as well as sharing experience, knowledge and analysis.

The constitution of an ISAC must be based on several premises:

- Confidence bonds between the participants with a policy of responsible release of the information;
- Establishment of a conduct code approved by all;
- Establish information sharing procedures and mandatory reports;
- The involvement of public and private sectors of the same area of intervention or geographic area;
- Must be self-sustained with regular results presentation and evaluation of performance;

- Clear definition of the ISAC role and relationship with the competent authorities;
- The development of the ISAC core services.

4.3.1. Reasons to create an ISAC

There are several reasons to develop an ISAC from the private and public perspective:

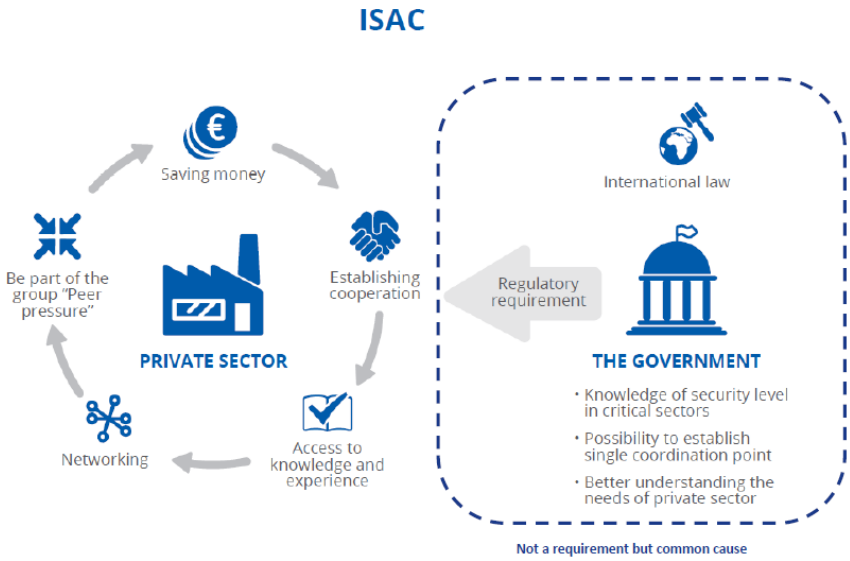


Figure 4-2 - Reasons for the creation of ISACs [70]

Table 4-1 -Private and public sector reasons for participation in ISACs [70]

PRIVATE SECTOR	PUBLIC SECTOR
Sharing knowledge about incidents and cybersecurity **It helps to raise the level of cybersecurity in the organisation which is a member of an ISAC and prevent/ respond to the incidents which occur.**	Knowledge of security level in critical sectors Being a member of an ISAC gives the public sector access to knowledge about the cybersecurity level in critical sectors. It also provides information about threats and incidents. This association is helpful as it enables them to fulfil their legal tasks better.
"Be part of the group" "Peer pressure." **Entities want to take part in an ISAC because it enables them to confront their ideas and experience with other organisations and learn from the best practices.**	Opportunity to establish a single coordination point Being a member of an ISAC allows the public sector to create a single coordination point, which has been proven to be very beneficial in the case of large-scale incidents. This fact enables them to fulfil their legal tasks better.
Access to knowledge and experience **For an organisation which is not so sophisticated in the field of cybersecurity, the ISAC is a fast and efficient way to get all the knowledge and expertise which usually takes a lot of time.**	Better understanding the needs of the private sector Thanks to close cooperation with the industry, public entities get a better understanding of the private sector, which has proven useful during setting up of new legislation and cybersecurity strategy. This fact enables them to fulfil their legal tasks better.
Networking **Being a member of an ISAC is the right way of networking and meeting people from different organisations. In the presence of an incident and when the gathering of information is needed, there is always a know-how way to network with the respective team.**	Demand of International Legislation
Better investment **The accumulated knowledge of the area will allow better investments and so spend less money assuring the cybersecurity standards.**	

4.3.2. Objectives of an ISAC

The CNCS has defined four goals to be reached by an ISAC [71]:

Table 4-2 - Portuguese ISAC Objectives [71]

To develop a trusted environment. In which there is responsible information sharing between the ISAC members.	To establish an active forum to identify the problems. That could compromise the cybersecurity of the sector.
To identify and develop mitigation measures concerning the threats detected.	Prevent cyberattacks to the sector, through the establishment of good practices and countermeasures.

4.3.3. The levels of participation on an ISAC, and the coordinator role.

To participate in the ISAC, the CNCS foresaw at least three levels of participation:

1) The facilitator: that is the CNCS or another representative organism in the sector (which in our proposed model would be the AMN);
2) The member: all the actors of the sector and;
3) The partner: an organisation, that is of interest to the ISAC, which participates in certain sessions to share information and participate in the development of work.

The coordinator of the ISAC is expected to challenge the other members to participate and share information. He also organises the agenda of the ISAC meetings, integrates the working groups and is responsible for the external communications of the ISAC.

The information shared in the ISAC concerns, for example, incidents, threats, vulnerabilities, mitigation measures, situational awareness, good practices, strategic analysis, among others. The information shared to the coordinator has a release policy associated, by the ISAC regulations. The CNCS TLP code (Traffic Light Protocol) suggests using a four-colour code: red, cannot be shared; yellow, only shared inside the ISAC; green, limited released, only to the community; and white, can be freely shared. In the model proposed, a more robust coordinator is envisaged with more tasks and responsibilities associated with this entity.

4.4. The proposed organisation

As mentioned before, the base organisation would be kept, introducing only cybersecurity standards and plans to be included on the already demanded SSP, PFSP and PSP; thus, no new organisation would be created from scratch.

According to the Decree-Law 49-A/2012, the security competence belongs to the DGRM, but the Decree-Law 226/06 states that the AMN supports DGRM in this role, coordinating all those involved in the security of the maritime spaces and port areas, under DGRM articulation.

Another factor to take into consideration is the territorial dispersion and proximity with the Maritime Community. The DGAM has a decentralised structure, as explained before, that through their local delegations applies the legal competences given by law to the Maritime Community. So, this structure gives them the operational advantage and privileged relation with the community to be able to support the DGRM and CNCS to help implement and ensure the compliance of cybersecurity regulations and norms in the Maritime Transport Sector.

Furthermore, the AMN already integrates the National Committee for Ports and Maritime Transports Safety, it must also issue its agreement to the PSP and it participates in the security inspections to harbours conducted by the DGRM.

These activities give the AMN an operational advantage to establish itself as a crucial player in the cybersecurity of the Maritime Domain, so this proposal is just following that bias.

We cannot forget that the solution proposed here will require a protocol between the AMN, DGRM and CNCS to provide the legal framework that allows the AMN to assume these functions of coordination and information sharing on the Maritime domain, centralising this information and relaying it to the CNCS and DGRM.

The ISAC Constitution would give a follow up to the NIS directive and would assure the cybersecurity coverage of the maritime transport, including inner waters maritime transport, specifying the maritime transport companies, the Port Authorities and Maritime Transport Operators.

4.4.1. ISAC of the Maritime Transport Sector

Considering what was explained previously, the proposal is based on the constitution of an ISAC (Information Sharing and Analysis Centre) for the Maritime Transport Sector, the AMN assuming the role of the ISAC coordinator, designated by the DGRM or by legislative revision, to assure cybersecurity in the maritime domain, with the following tasks, among others:

- Being the central units that receive the events from the different SOCs of the Maritime Sector;
- Making the responsible discloser and dissemination of the relevant information between the Maritime Community SOCs and actors;
- Coordinating the response to events, giving the first support to the SOCs, including technical if needed;
- Making the liaison with the CNCS:
    - To update the Maritime Domain cyber situation;
    - To report all events and responses given;
    - To request support to respond to events, and, if needed, technical or forensic support;
- Giving specialised support to the operators to establish and maintain cybersecurity organisation and standards;
- Running cybersecurity helpdesks in the main harbours (Lisbon, Oporto [Leixões], Sines, Faro, Ponta Delgada and Funchal);
- Conducting inspections to the Maritime Transport Sector operator to assure the implementation of the SSP, PFSP, PSP:
- Coordinating the execution of national cybersecurity exercises in the Sector of the Maritime Transports, in coordination with the CNCS and DGRM.

The AMN would be the Coordinator of the ISAC for all the Maritime Domain operators, like the Bank of Portugal for the bank sector. That would ease the CNCS and the DGRM load and would permit a faster and more specific answer to cybersecurity maritime events.

The function that we propose is wider than that of a traditional ISAC, due to the fact that our maritime domain is vaster and more complex than the traditional areas. Some of the maritime specificities are: the sea is the main actor of the economic development; there is a similarity between Maritime / Digital

domains; the Maritime domain is a cross-sectoral domain; there is an imperative need of an information-sharing environment. [72]

	Maritime	Digital
Dimension	80% of earth	Unlimited
Legal	Weak international regulation UNCLOS	Limited inernational Regulation GDPR
Economical	90 % of international Trade Stable	50 % of international transactions Permanent growth
Environment	Unpredictable: Sea state, Wind, Salt, Physical dangers	Unpredictable: Virtuality,
Threat	Illegal activities and handlings, Piracy, Terrorism	Global Scope of Cyberthreats Illegal activities focused on goods
Focus	Share information (IFC) Acting capacities = States	Prevent & Share information Coordinate action

Figure 4-3 - Maritime / Digital similarities [72]

The final goal could be the establishment of a Maritime Cybersecurity Coordination Centre, proposed as a future work, more than an ISAC to establish a Maritime CERT. For that, we need a more robust legal base, a taxonomy, a Maritime Governance, a technical base and, in the top of this, a CERT-M. This CERT-M would coordinate and support regional SOCs to react to events and issue mitigation measures through the ISAC.

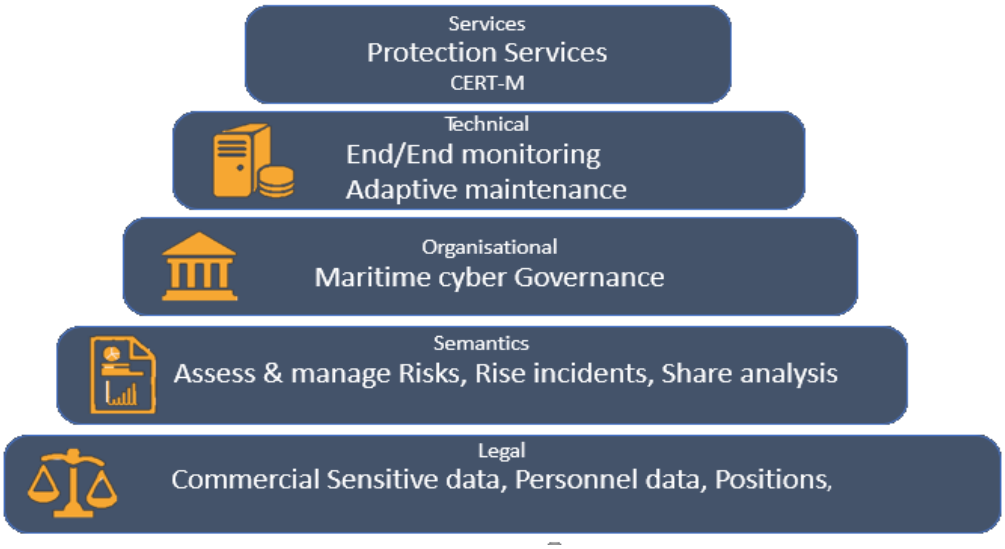


Figure 4-4 – CERT-M Development Pyramid [72]

4.4.2. Key elements and Plans

These definitions are adapted from [34, 60]:

- Ships' Cybersecurity officer (SCySO) - The person or persons tasked to manage and coordinate the cybersecurity of a ship. For larger fleets, the SCySO usually reports to the Company's Chief Information Security Officer (CISO) or CSO, for smaller fleets he is likely to report to the Company's Head of Security.

- Cyber Security Assessment (CSA) - The relationship of the CSA to the ship security assessment (SSA) and the ship security plan (SSP), required by European legislation and the ISPS Code, Part B, paragraphs 8.1 to 8.10, provides guidance on aspects to be included in the SSA, which comprise computer systems and networks. Assessing the cybersecurity of ship assets requires specialised knowledge and expertise, and, as such, it is recommended that suitably qualified and experienced individuals assume the preparation of the CSA and CSP.

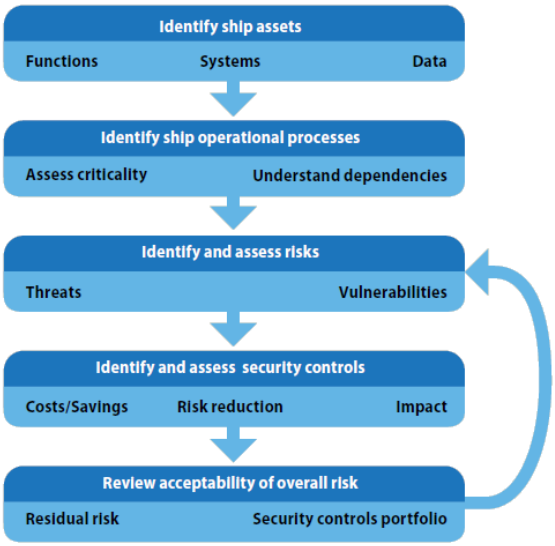


Figure 4-5 - CSA Development on a Ship [34]

- Cyber Security Plan (CSP) - The ship security assessments form the basis of the security plans for the ship. These plans should address the physical and personnel issues identified in the relevant evaluation through the establishment of appropriate security measures intended to minimise the probability of a breach of security and the consequences of potential risks. It is intended that wherever applicable, the CSP will build upon the existing ship security plan (SSP) and may be an annex to it.

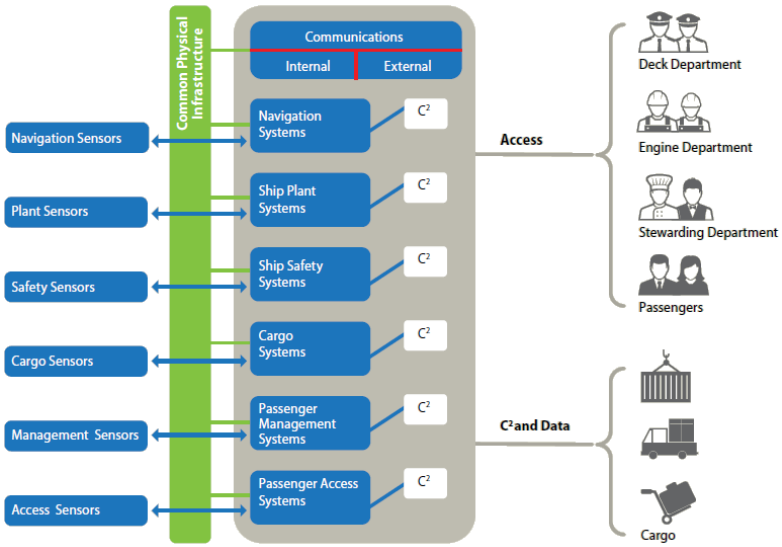


Figure 4-6 - Cybersecurity on a Ship [34]

- Cybersecurity officer (CS officer) - The person or persons tasked to manage and coordinate the cybersecurity in a port/port facility. For larger ports, the CS officer usually reports to the chief information security officer (CISO). For smaller ports, the role is expected to report to the Head of Security.
- Port Facility / Port Cybersecurity Assessment (CSA): The port and port facility should first assess each of the vulnerability and countermeasures identified in the final port/port facility assessment reports to establish if cybersecurity implications are arising from them. It is intended that, when suitable, the CSA should build upon the existing security assessments.

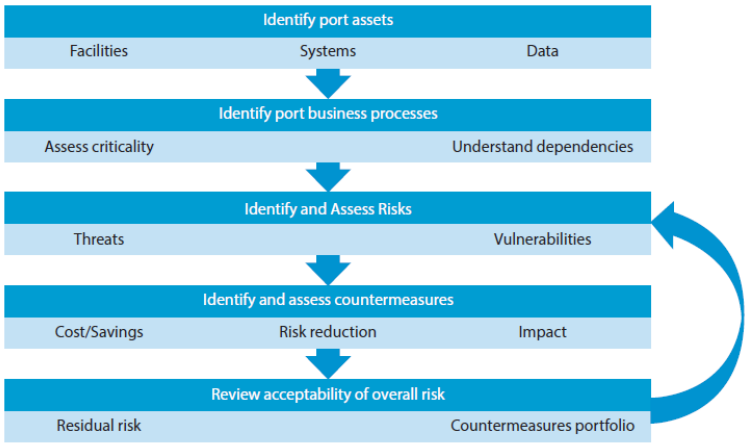


Figure 4-7 - CSA Process [60]

- Port Facility / Port cybersecurity plan (CSP): The security assessments form the basis of the security plans for the port and port facilities. These plans should address the issues identified in the relevant evaluation through the establishment of appropriate security measures designed to minimise the probability of a breach of security and the consequences of potential risks. It is intended that, when suitable, the CSP will build upon the existing port facility/port security plan (PFSP/PSP).

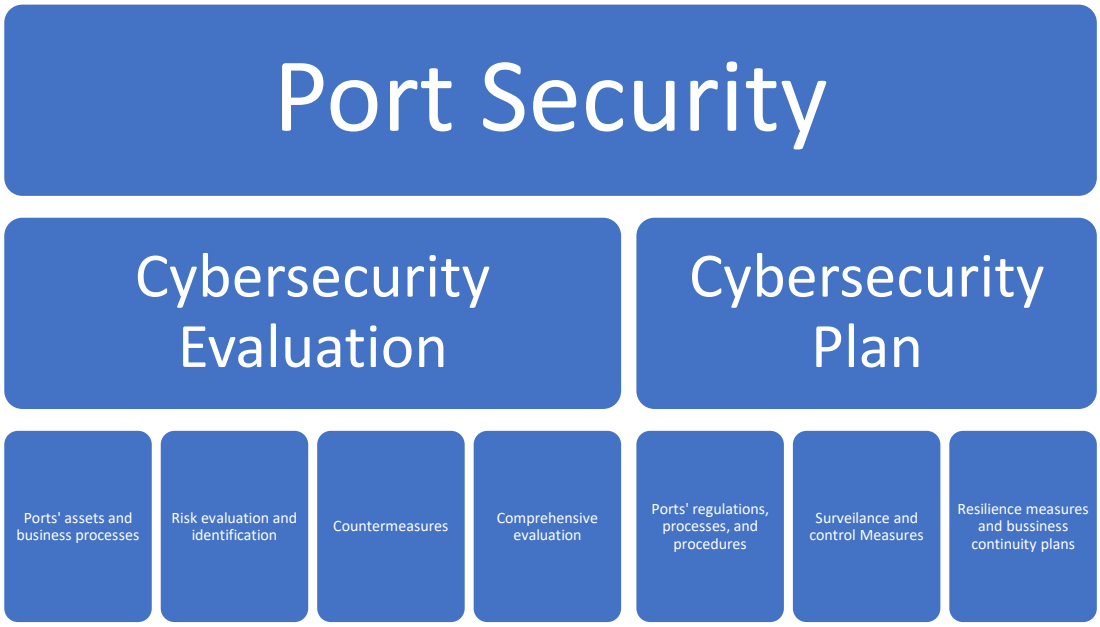


Figure 4-8 - Port Cybersecurity

The DGRM should promulgate the education requisites for the key players after the proposal of the CNCS after AMN issued his opinion.

The approval of the CSA and CSP should be done by the DGRM after CNCS and AMD issued their opinion. In the case of the Port Facilities and Ports, the CCPP also must issue an opinion on the cybersecurity assessment and plan.

4.4.3. Inspections on the cybersecurity measures

It is necessary to conduct inspections to assure the implementation and the updating of the Ships / Ports Facilities / Ports Cybersecurity Plans that should be included in the SSP, PFSP and PSP;

AMN specialised inspection teams should conduct the inspections of ships, port facilities and ports, in articulation with the DGRM, giving them results of the inspections and informing the CNCS. The inspectors must have a certification issued by the CNCS for conducting such inspections and the competence delegated by DGRM through a signed protocol. The inspections, if possible, should co-occur with the security inspections in the other areas.

To facilitate the inspection process and the upkeep of the CSP, in the designated helpdesks, pre-inspection teams and teaching team must be available to give support to ships, port facilities and port operators.

Those helpdesks should also provide support on training plans and, if requested by the operator, conduct cybersecurity exercises and validations to a specific ship / port facility/port.

A national cybersecurity drill should be planned and performed at least once a year.

4.5. Inferences

Following the analysis conducted in the previous chapters, we concluded that the model proposed should be implemented using the existing organisation to assure the security of the maritime domain.

Accordingly, we proposed a model using the AMN as the focal point of the cybersecurity of the maritime domain, keeping up her role of supporting the DGRM in the coordination of the maritime security and maintaining its law enforcement tasks, that can be extended to encompass the cybersecurity aspect in the maritime domain security.

To accomplish this task, the AMN should establish a protocol with the CNCS and the DGRM, to have recognised expertise to become the ISAC of the Maritime Transport Sector of CNCS and assure the necessary legal competence through DGRM.

Also, to provide adequate support and create a proximity feeling to maritime operators, it should create cybersecurity helpdesks in the main Portuguese harbours.

The AMN must assure certified inspection teams to verify the implementation of the cybersecurity part of the SSP/PFSP and PSP.

The authority for the approval of the CSA (annex of the SSA, PFSA, PSA) and CSP (annex of the SSP, PFSP, PSP) would be kept by the DGRM after CNCS and AMN issued their opinion.

It is necessary to include, in the minimum contents of the security plans and assessments, a cybersecurity component as a mandatory field. These actions must be done with a legislative process complemented with technical norms and standards. These documents can easily be adapted from the ones used in other friendly countries that have already implemented them, e.g. IET Standards for Cybersecurity.

With this simple process, we can quickly implement the cybersecurity factor in the Maritime Transport Sector, verify its implementation, and provide minimum standards of education, training and routine internal verification.

The proposed model does not recommend a disruptive organisation, on the contrary, it fosters the adaptation of the current one, implementing the cybersecurity competence to the coordinating security entity of the SAM, the AMN, widening the security scope coordination and verification of implementation. This proposal is of easy implementation and it is based on the already present and accepted competencies.

To validate this model inquiries to the expertise elements of the Maritime and Cybersecurity Community were conducted; this will be addressed in the next chapter.

This chapter is the answer to the research question and the base for validation of the fourth hypothesis that now needs to be validated. This validation will allow the corroboration of the fourth hypothesis and of the thesis itself.

5

Validation

It is the purpose of this chapter to make the validation of the proposed model and the results.

5.1. Validation of the proposed model

The proposed model was validated by conducting a questionnaire to subject-matter experts, using the results to adapt to the model.

5.2. Identifying the target audience for the questionnaires

To have a resulting balanced model with contributes of experts belonging to all the sectors of the maritime domain, facilitating its acceptance and future implementation, we needed to identify the target audience for the questionnaire and define validation rules for the answers.

The maritime domain is a broad spectrum of sectors and role players, encompassing, e.g., academia, law enforcement, AMN, DGRM, ship companies, seafarers, port administrations, port operators, insurance companies, among a lot of other players. We also decided to include in that universe the experts that performed duties related to the maritime security sector in the last seven years, considering that in the Amsterdam event that occurred in 2011 [60] raising cybersecurity issues in Maritime Transport Sector, these experts were the first ones to face the problem and have experience in dealing with the matter. Also, the ENISA issued its first report concerning the cybersecurity of the maritime sector [38] alerting the member states for the need to take urgent measures ensuring cybersecurity in the sector and for the disastrous consequences of an attack in this vector for national and EU economy.

Also, to have a better analysis base, we divided the target audience into groups that have the same synergies and objectives. Therefore, we used a probability sampling method, the Cluster Random Sampling. Cluster sampling is defined as a sampling method where multiple clusters of people are created from a population where they are indicative of similar characteristics and have an equal chance of being a part of the sample. In this sampling method, a simple random sample is created from the different clusters in the population. [73]

The analysis is carried out on a sample which consists of multiple sample parameters such as demographics, habits, background — or any other population attribute, which may be the focus for con-

ducting the research. This method is usually performed when groups that are similar yet internally diverse form a statistical population. Instead of selecting the entire community of data, cluster sampling allows the researchers to collect data by bifurcating the data into small, more effective groups [73]. So, we divided the target audience for the questionnaire into the following groups:

Table 5-1 - Division in Groups of the Experts

Group	Entities
Maritime Authorities	AMN DGAM Port Captaincies Maritime Police DGRM AMT
Academia	Nautica School Naval School Fishing Masters School Rating School Law Faculty of Lisbon Technical Superior Institute of Lisbon Security Officer Formation Schools
Maritime Community	Ship Companies Ship Owners Ship Operators Ship Handlers Insurance Companies Merchant Navy Officers Association Merchant Navy Ratings Association Shipyards Maritime Handlers Insurance Companies Ship Chandlers (…)

5.3. The Questionnaire Structure

The questionnaire was divided into six groups of questions, each with different goals.

5.3.1. The Demographic Questions

This group of questions had the objective of establishing the profile of the person that answered the survey.

Questions were asked to know the gender, the age, the education, the expertise and field of experience of the inquired person and assert if that profile would condition the answers.

5.3.2. The Legal Framework concerning the Cybersecurity in Portugal

The second group of questions had the objective of perceiving how the Maritime Community evaluated the existing legal framework in Portugal and the Maritime Domain in particular.

5.3.3. The Validation of the ISAC need

The third group of questions had the objective of determining if the target audience saw the need for the edification of an ISAC for the Maritime Transport Sector. This section finished asking if it was acceptable that the AMN would assume the role of coordinator of that ISAC.

5.3.4. Cybersecurity Definitions in Maritime Transport Sector acceptance

The fourth group of questions had the objective of understanding if the inquiries accepted a group of chosen definitions that targeted to include the cybersecurity aspect to the already existing security plans and the definition of roles for cybersecurity. This section finished with the question of accepting the adaptation of two reference UK publications of cybersecurity in the maritime domain.

5.3.5. The role of the Cybersecurity Helpdesks

The fifth group of questions had the objective of knowing if the target audience agreed on the constitution of helpdesks to support the maritime community into building up resilient cybersecurity standards and on what should be their role.

5.3.6. The Private Companies role

The sixth group of questions had the objective of understanding if the inquiries agreed that private cybersecurity companies could support the elaboration and verification of the CSP of ships, ports and port facilities. This group finished with a question on the level of approbation of the CSP, which should be the same as the SSP, the PSP and the PFSP.

5.4. Validation Rules

For validating the sample for the questionnaire, it was defined that we would need a 95% confidence level with a 7% sample error margin.

To be able to know the number of correctly answered questionnaires we needed to have, we had to define the sample universe for the six groups and, based on the sample validation criteria, we found the required number of validated questionnaires.

The calculations of the needed sample were conducted based on [74]:

$$n = \frac{Z_{\alpha/2}^2 \cdot p \cdot q}{E^2}$$

Where:

n = Number of individuals that compose the sample

$Z_{\alpha/2}$ = Critical value that matches the wanted confidence level

p = Population proportion of the individuals that belong to the category that we are studying

q = Population proportion of the individuals that do not belong to the category that we are studying (q = 1 - p)

E = Error Margin that identifies the maximum difference between the sample proportion and the population proportion.

So, for a population of 100 targeted individuals, we need to have 66 validated answers to the questionnaire, as shown in Figure 5-1 [74]:

Finite population

Dimention of the target population	**100**
Confidence Level	95,0%
Sample Error	7,0%
Critical value	1,96
Required Sample Error	**66**

$$n = \frac{\hat{p}\hat{q}}{\frac{B^2}{z^2} + \frac{\hat{p}\hat{q}}{N}}$$

Figure 5-1 - Needed Sample Calculation - Example

The total universe of each group was obtained by analysing the organograms, or inquiring the addressed organisations, and was limited to the specialist personnel on security or cybersecurity of the company, the decision-makers concerning those subjects and the directors that handle the organisation's institutional answers and strategic decisions. The results obtained were the following:

Table 5-2 - Universe of Questionnaires and Required Answers

Group	Sample Universe	Minimum Sample Required
Maritime Authorities	85	59
Maritime Community	707	153
Academia	27	24

5.5. Validating the Questionnaire

In the questionnaire, in Appendix 2, there are two primary types of questions, the first type is constituted with questions already validated by experts and previous academic works, ten questions in a universe of 43, and the other ones required a validation process.

To validate these questions two validation tests involving two distinct target groups were performed: the first one was done by 80 cadets of the 4th and 3rd years of the Naval School and the second test was done by 30 officers of the Naval Staff.

After evaluating the results of the first run and attending the doubts raised by the participants during the questionnaire execution, the questions, that needed, were rephrased to take out any misleading or ambiguity of it. Afterwards, the questionnaire was rerun by the second group that confirmed the validity of the questions and the survey was considered validated and ready to be deployed.

5.6. Proceeding with the Deployment of the Questionnaire

After having defined the sample universe, it was necessary to proceed with the questionnaire. For this task, the author searched the e-mail contacts of the target groups and deployed the poll based on a commercial web-based survey tool. "*QuestionPro*".

The results were the following:

Table 5-3 - Results of the Questionnaires

Group	Sample Universe	Minimum Sample Required	Sample Received
Maritime Authorities	85	59	72
Maritime Community	707	153	308
Academia	27	24	4

Achieving the minimum validated questionnaires to assure the defined validation criteria to all the groups we proceeded to the analysis of the answers.

5.7. The Reliability of the Questionnaire

To test the reliability of the questionnaire, we used the Cronbach Alpha reliability measure. Cronbach's alpha reliability [75] is one of the most widely used measures of reliability in the social and organisational sciences. Cronbach's alpha reliability describes the reliability of a sum (or average) of k measurements where the k measurements may represent k raters, occasions, alternative forms, or questionnaire/test items. When the measurements represent multiple questionnaire/test items, which is the most common application, Cronbach's alpha is referred to as a measure of "internal consistency" reliability [76].

$$\alpha = \frac{k}{(k-1)} \times \left[1 - \frac{\sum_{j=1}^{k} S_j^2}{S_T^2} \right]$$

Figure 5-2 - Cronbach formula [77]

Where k is the number of items of the instrument, $S_j^2 = \frac{1}{n-1} \sum_{i=1}^{n} (X_{ij} - \bar{X}_j)^2$ is the item variance of j (j=1,…,k) and S^2_T is a variance of the totals of the chosen scale.

For the validation questionnaire, the Cronbach α is of 0,75, which indicates an acceptable consistency and reliability of the survey.

Also, we verified if the answers had the same statistic distribution; if so we could eliminate the questions more similar to increase the Cronbach α. The same issue was confirmed when we performed several tests to compare the answers to the questions: the paired T-test, McNemar's test for frequencies comparison and the Crochan's Q test for binary variables comparison (agree versus not agree). Also, we performed the Friedman test (p-value<0.005) and Kendall's coefficient of concordance test (p-value<0.005). All tests led to the same conclusion: the distributions of considered questions are not the same. Notice that the Spearman correlation coefficient leads to significant relations between some questions. Also, Friedman's test supports such an association (p-value<0.005).

5.8. Analysis of the Questionnaires Results

One important fact is that for the same organisation, sometimes, several e-mails were sent targeting different people in the hope that one would answer, but often the organisation contacted the author stating that they would centralise the answer on their cybersecurity expert so only one questionnaire would respond for that organisation.

We must consider that of the 707 e-mails sent to the Maritime Community about 400 targeted different organisations.

Also, in the Maritime Authority Group, we only received answers from the AMN connected addresses, none were received of the DGRM, which limited the results obtained in this group to a single view perspective, but also relevant to global results.

Slightly disappointing was the Academia Group's response, for, as this is an academic work, we expected a good participation from this group, but it was quite the opposite: of the 27 e-mails sent we only obtained four answers, which do not validate the group's position. These answers were only taken into account for the global results considerations.

The participation in the questionnaire, not considering the Academia Group, allowed passing the sampling error from 7% to 5%. The minimum participation in obtaining the 5% sample error is:

Table 5-4 - Required Answers for a 5% Sample Error

Group	Sample Universe	Minimum Sample Required	Sample Received
Maritime Authorities	85	70	72
Maritime Community	707	249	308
Academia	**27**	**25**	**4**
Total	819	344	384

So, we can consider that in these groups, as in the total deployment of the questionnaire, the Sample Error was of 5% and not the 7% initially targeted.

5.8.1. Demographic Questions

Concerning the analysis of the group of demographic questions, we can draw the following conclusions: we noted that the average age of the people answering the questionnaire was above 40. This associated with the fact that more than 90% have a higher education (PhD, masters or Licentiate — a former degree that is equivalent to the actual Masters) shows that, probably, the people that answered the questionnaire were of medium or high-level administration of the companies.

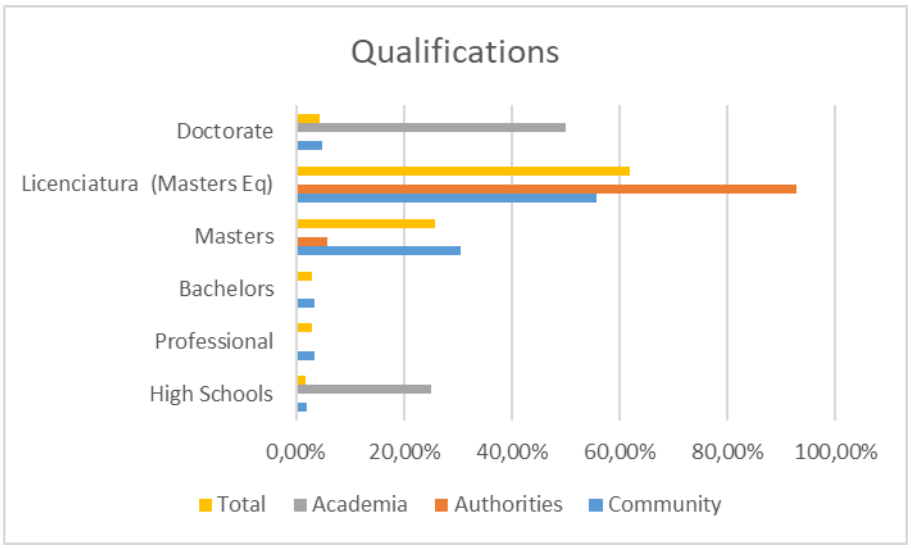


Figure 5-3 - Qualification of the Inquiries

We also observed the low level of female presence in the cybersecurity area: less than 20%. Considering their professional expertise, we noticed that, excluding the maritime authority group, those who answered were all Navy Officers, ranging across many expertise's, but mostly belonging to the security and cybersecurity branch. Furthermore, almost 50% were performing tasks of information security and technologies applied to the Maritime Domain.

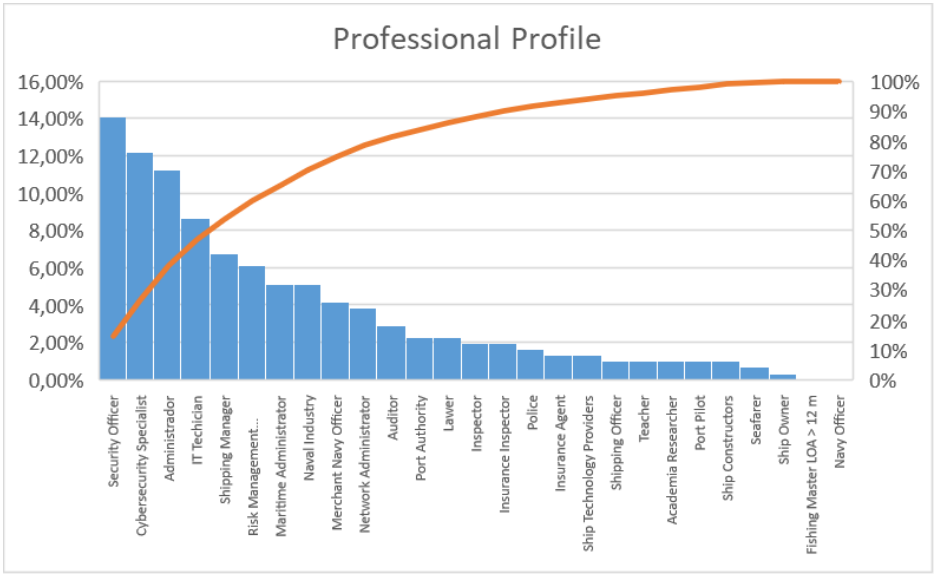


Figure 5-4 - Professional Profile of the Inquiries

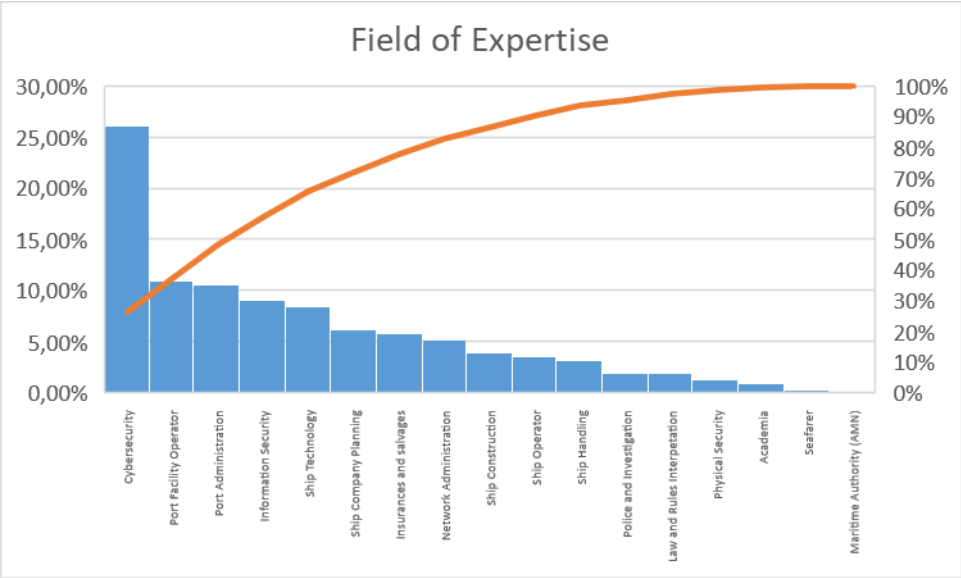


Figure 5-5 - Field of Expertise of the Inquiries

The companies that they worked for were mostly port facilities operators, navigation companies and port administrations.

We can conclude that the companies that received the questionnaire sent it to be answered by the company's security or cybersecurity expert or to the person responsible for it. That shows the importance this subject has to the Maritime Domain Community.

5.8.2. The Legal Framework concerning Cybersecurity in Portugal

We noticed that a considerable part of the surveyed did not know how to answer this group of questions, for about 20% responded that they did not know how to answer. Nevertheless, more than 70% of the inquired answered that the cybersecurity legal framework concerning the maritime domain was not enough, and the general cybersecurity legal framework in Portugal was enough. Only a small number of answers went out of the enough or not enough possibilities, but almost 10% answered that a legal framework for the cybersecurity in the maritime domain was inexistent.

Nevertheless, after conducting the T-tests on the questions related to the Legal Framework, we obtained a p-value<0,05 confirming that the questions had answers significantly different, so as not to be excluded in the statistical analysis.

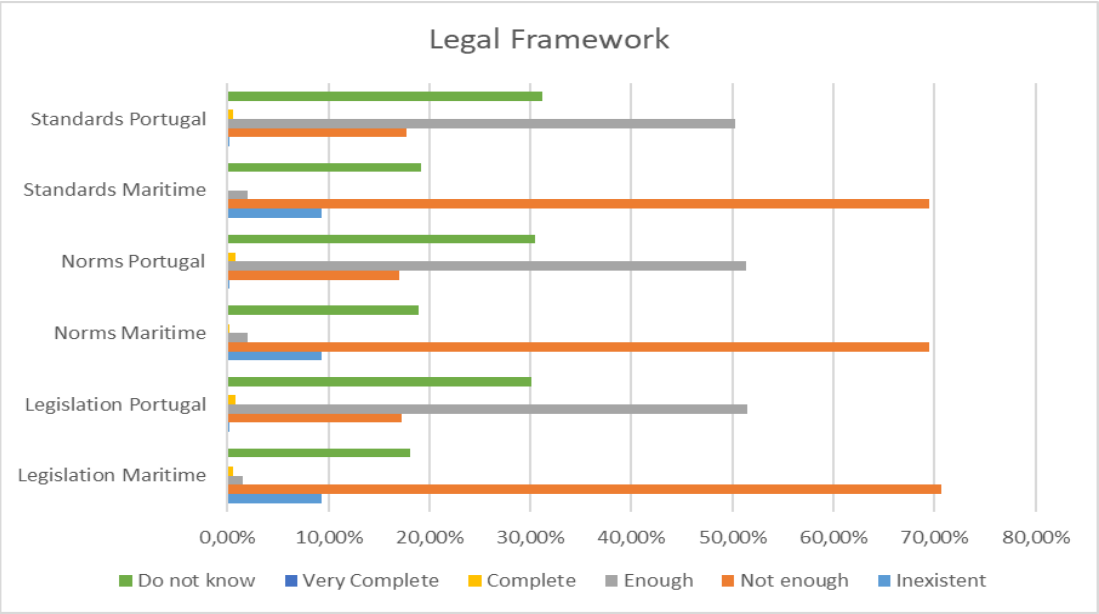


Figure 5-6 - Legal Framework Perception

So, we can conclude that the Maritime Community feels the need of clarification or edification of a cybersecurity legal framework considering specifically the Maritime Domain. This need should quickly be addressed by the ISAC coordinator in conjunction with the DGRM and CNCS.

5.8.3. Validation of the ISAC need

In this group of questions, we could see that more than 95% of the surveyed agreed on the constitution of an ISAC for the Maritime Domain, responsible for the coordination and the information dissemination throughout the sector.

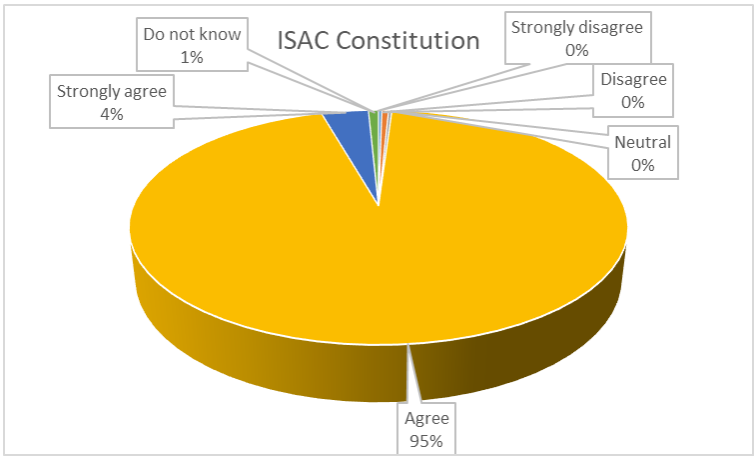


Figure 5-7 - ISAC Constitution Acceptance

Concerning the issue of choosing the AMN as the entity in charge of the coordination of this ISAC, in close articulation with the DGRM, 68% responded positively. The negative answers were divided, in more or less 50%, between DGRM and CNCS to assume that role.

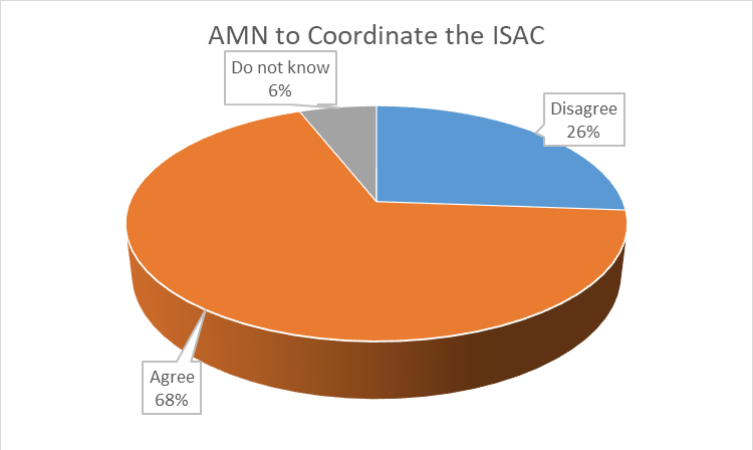


Figure 5-8 - AMN Coordination of the ISAC Acceptance

So, we can conclude that the Maritime Community desires the constitution of a Maritime ISAC and in a great extent agrees that AMN could assume the coordinating role of that ISAC.

5.8.4. Cybersecurity Definitions

Considering this group of questions, we could observe that more than 90% of the surveyed concur with the definitions suggested and with the inclusion of the cybersecurity component in the SSP, PFSP and PSP. We can see that the participants had identical and similar answers to most of the options. All T-tests were not significant.

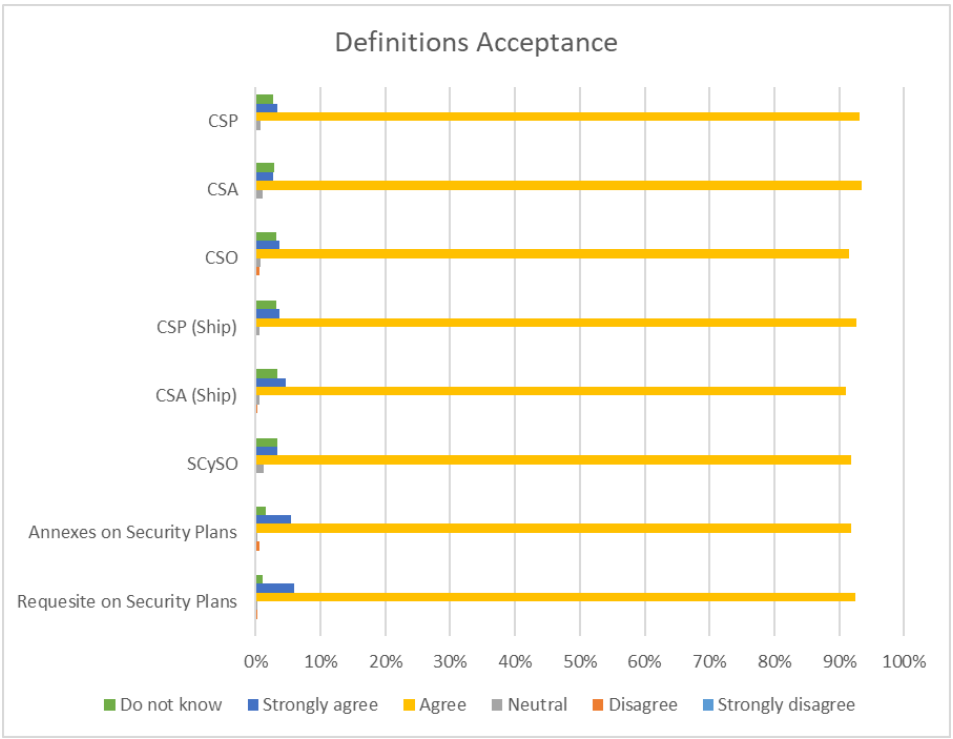


Figure 5-9 - Definitions Acceptance

Furthermore, 61% of the inquired knew the reference publications, IET Standards concerning the cybersecurity of ships and harbours, and 60% of those agreed that these publications should be translated and adapted to be applied in Portugal. Notice that more than 30% of the participants declared neither agreeing nor disagreeing.

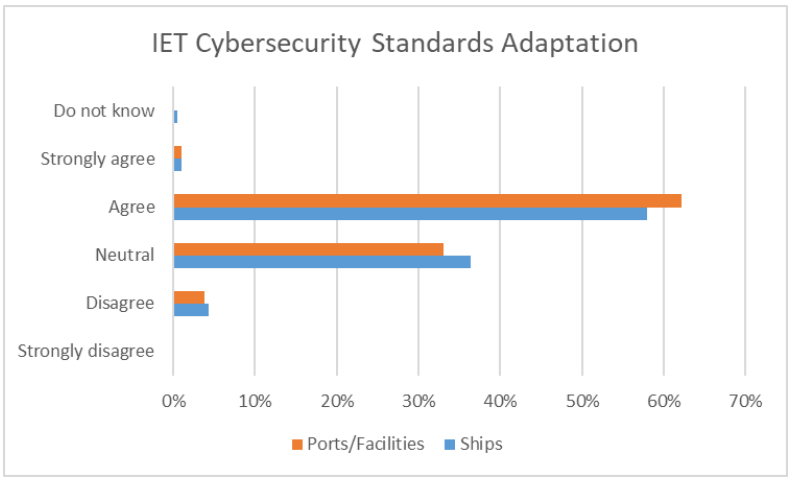


Figure 5-10 - IET Standards Acceptance

So, we can conclude that it is paramount to include the cybersecurity issue in the elaboration of the SSP, the PFSP and the PSP, being integral part of these security plans. Also, the coordinator of the ISAC can use the referred IET Standards to apply to Portuguese reality.

5.8.5. The Role of the Cybersecurity Helpdesks

More than 99% of the respondents agreed on the constitution of helpdesks to support the implementation of cybersecurity in the Maritime Domain.

Also, more than 95% of the surveyed agreed that these helpdesks would support the Maritime Community in the preparation for inspections, in the elaboration and execution of the training plans and the conduction of exercises.

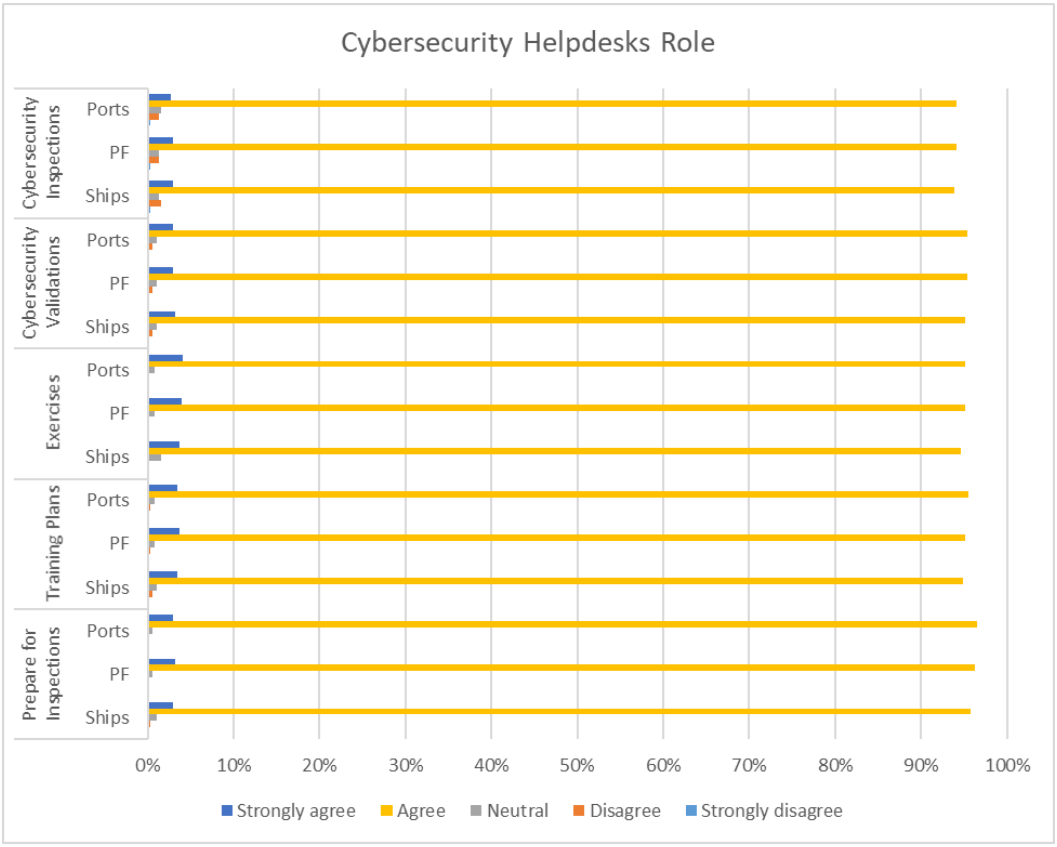


Figure 5-11 – Helpdesks Role

Another relevant fact is that more than 94% of the inquired agreed that these helpdesks should have inspection teams and conduct inspections to the ships, port facilities and ports to assure the implementation of the cybersecurity plans.

So, we can conclude that the Maritime Community agrees on the constitution of the helpdesks and on these helpdesks having the competence to conduct inspections and to assure the cybersecurity of the sector.

5.8.6. The Private Companies Role

The role of private companies in the cybersecurity of the sector has an entirely different answer scope in the Maritime Community Group and among the Maritime Authorities. In the Maritime Community Group more than 90% agree on the certification of private companies to elaborate the SSP, the PFSP and the PSP, to conduct exercises and verification inspections. Differently, in the Maritime Authorities Group only 50% agree and about 35% disagree with this.

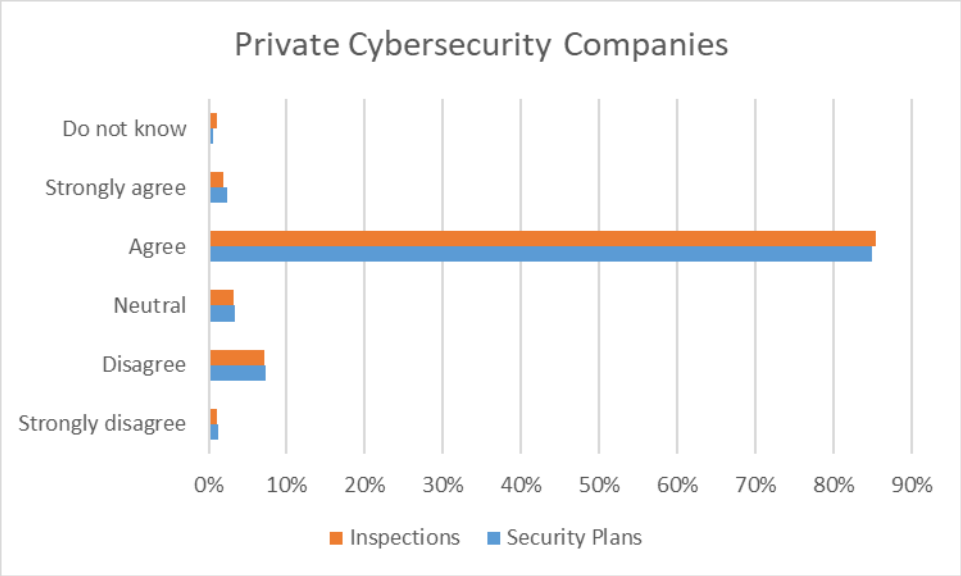


Figure 5-12 - The Private Companies Acceptance

But in the end, we can conclude that the Maritime Community as a whole sees the critical role that the private cybersecurity companies have or may have in assuring the cybersecurity of the Maritime Domain.

5.9. Inferences

From the questionnaire results, we can draw several important conclusions.

The Maritime Community:

- Has a concern for the cybersecurity of the sector, as may be seen in the fact that they selected as respondents those in a high level of administration;
- Feels that the legal framework concerning cybersecurity of the sector is not enough and needs a rapidly clarification or build-up;
- Agrees on the constitution of an ISAC and on the choice of the AMN for the coordination role of this ISAC, in articulation with the DGRM;
- Agrees that the cybersecurity component must be included in the actual security plans and that foreign standards could be adopted to increment maritime cybersecurity;

- Welcomes the constitution of helpdesks to support the cybersecurity build-up of the sector and agrees that these helpdesks could have teams with the competence to inspect the cybersecurity standards of the sector;
- Agrees on the importance of involving the private cybersecurity companies on the build-up of the Maritime cybersecurity.

All these conclusions, with significantly high rates of approval, lead to the adoption of the proposed model in this thesis, and so we can conclude that the Maritime Community approves the proposed model.

6

Conclusions

In this chapter the validity of the model is explained, as well as the way to implement it.

6.1. From a research question to validation

In chapter one, we established the following research question: *What is the organisational model for assuring the cybersecurity in the Portuguese Maritime Domain and ensuring the Cybersecurity Law compliance?*

To be able to answer to this question we had to scrutinise several hypotheses, through chapters 2 to 4. This led us to develop the proposed model in order to proceed with its validation, in chapter 5.

Also, we thoroughly reviewed the "*state of the art*" and, as a support base to elaborate the proposed model, we built an analysis model based on three major theories used in this type of subjects related to organisation models, namely those applied to new technologies: the "Grand Strategy Theory", the "Activity Theory" and the "Actor-Network Theory". The combination of these theories allowed us to establish a strong scientific basis to analyse the existing organisation models and to be able to build a new one upon the analysis results of the combined model.

The verification of the hypotheses throughout the thesis developed in the following way.

6.1.1. The first hypothesis

The first hypothesis was the following "*The European models for cybersecurity are more adequate for the Portuguese reality than others*".

To prove this sentence, we analysed, in chapter 2 (detailed in the Annex "State of the Art"), the "state of the art" in four countries that were chosen using scientific criteria: three of them from the EU, the fourth being the USA. We verified the deviation of the USA organisation from the EU countries and the better adaptability of the models of the EU countries. One of the main reasons encountered was the similarity of the legislative framework in EU countries due to fact that EU Directives are mandatorily transposed to national law.

Also, another crucial aspect is the role of the organisational culture and organisational structure that is the main issue to ensure a fast adaptation and acceptance of a new organisational structure. Also, the European differs from the non-European ones.

This was fully explained in chapter 2 (detailed in the Annex “State of the Art”) and these are the factors that validate the first hypothesis.

6.1.2. The second hypothesis

The second hypothesis was the following: “*The EU legislative framework has more influence on the adopted model to ensure cybersecurity in the EU countries than the other factors*”. This question was answered throughout Chapter 2 (detailed in the Annex “State of the Art”).

The main issue is that the EU countries must transpose the EU legislation to the national one, even if they can make adaptations to their reality and law.

Due to this fact, the legislative framework concerning safety and security of the maritime transport sector is similar in all EU countries. Also, the implementation of the NIS directive in all the EU countries in 2019 homogenised the cybersecurity approach of the EU, and so we can conclude that the EU legislative framework is the basis for the security and cybersecurity of the maritime domain in EU.

These facts are very well demonstrated in the analysis made at the end of each country’s “state of the art” sub-chapters. Due to this evidence, we consider that the second hypothesis is also validated.

6.1.3. The third hypothesis

The third hypothesis was the following “*Adapting the actual maritime domain security organisation so as to include the cybersecurity aspect is more efficient and quicker to implement than raising a completely new organisation*.”, this hypothesis was also answered in chapters 2 (detailed in the Annex “State of the Art”) and 3.

We could see that all the countries adopted the existing security and safety organisation for the maritime domain to implement the cybersecurity factor. All of them considered that the cybersecurity is one more factor for the safety and security of the maritime transport sector.

Considering the analysis conducted in chapter 2 (detailed in the Annex “State of the Art”) and comparing it with the Portuguese reality we could conclude that the best way to implement a credible organisation for the cybersecurity in Portugal is through the existing organisation, implementing regulations and verification mechanisms to ensure that cybersecurity is implemented in the maritime domain by the various actors concerned with it.

To achieve this, all that is required is the adaptation of the existing organisation to the cybersecurity issue.

6.1.4. The fourth hypothesis

The fourth hypothesis was the following: “*The leading entity to coordinate the cybersecurity in the maritime domain should be an organism specialised in the Maritime Domain with a cybersecurity background and an established cybersecurity organisation rather than other with no cybersecurity experience or expertise*”. This hypothesis was validated in chapter 4, with the analysis and considerations to build the proposed model, and in chapter 5, with the validation of the model itself.

In chapter four we analysed the various organisms that could assume this role and, considering the existing organisation, the EU cybersecurity framework and the experience and operational status of those organisms, we developed a model afterwards validated by a survey to the main role-players of the maritime domain.

With this validation, we considered that the hypothesis was validated together with the model itself.

6.2. The validation

The validation process and the results are dealt in chapter 5 of this thesis.

Contrary to what we expected, the questionnaire was widely answered by the maritime community demonstrating the actual degree of concern of the community with cyberspace security and the impact and influence of the digital factor on the Maritime Transport Sector.

The validation achieved was fully described in chapter 5, and we can conclude that the model proposed was validated by the maritime community and should be implemented in Portugal.

6.3. The functional organisation to address cybersecurity in the Portuguese Maritime Domain

In chapter 4, we answered the research question, establishing a model of the targeted functional organisation, and in chapter 5, we validated that model. Due to this, we can state that the objective of this thesis was achieved with the establishment of a valid model for a functional organisation to address the cybersecurity in the Portuguese Maritime Domain.

6.4. Way Ahead

In parallel with the Maritime-ISAC implementation, 5 central SOCs should be created by regions located in the main harbour areas:

- Leixões SOC responsible for the north area;
- Lisbon SOC responsible for the central area;
- Sines SOC responsible for the south area;
- Ponta Delgada SOC responsible for Azores Islands;
- Funchal SOC responsible for Madeira Islands.

All these SOCs would report the events to an M-CERT. This M-CERT would coordinate and support the regional SOCs in reacting to events and issuing mitigation measures through the ISAC.

We can say that the implementation of the M-ISAC is the first step to the implementation of a robust organization to assure the cybersecurity of the maritime domain. After this first step is taken, it is crucial to proceed to the next one, which is to create the M-CERT, possibly with the same coordinator organism than the ISAC.

6.5. Future Work

6.5.1. Sectorial CERT

The implementation of an ISAC for the Maritime Transport Sector, with a more robust role in the implementation, assurance, coordination and verification procedures than a normal ISAC, should lead to the future implementation of a sectorial CERT for this sector led by AMN, or even a further and more ambitious organisation.

There is a French proposal to create a European Maritime Cybersecurity Coordination Centre, and for the interlocution with this new player, Portugal and the other EU countries should establish a similar national organisation.

The act of constituting this organisation is a fundamental step to assure the safety of this specific domain because of the unique maritime specificities, the vast domain (from certification to recovery), the need of an EU coordinated approach in an international environment. Also, this will bring the benefit of sharing parallel costs (certification, coordination) and having the possibility of establishing a Maritime capacity (M -CERT).

The study to establish a Portuguese Maritime Cybersecurity Centre should be the follow-on effort to this work.

6.5.2. Conduct an in-depth ANT analysis to the Cybersecurity Organisation

Due to the complexity of this analysis, we believe that a follow-on work to this thesis would be a detailed ANT analysis of the Cybersecurity Organisation of the referred countries.

That would allow us to establish a scientific relationship and encounter improvement suggestions to the proposed model or even suggest a Master organisation for the nations to adopt, considering the specificities of their own country.

Doing this analysis would be challenging work but it could bring significant results and conclusions.

6.5.3. Promulgation of Support Documentation

The existence of support documentation for the maritime community to be able to implement the cybersecurity requirements correctly and to be aware of the usefulness of its implementation is paramount to achieve safer cyberspace in the maritime domain.

Thus, it is necessary to develop that support documentation, based on the doctrine to be promulgated, on the normative and good practices in cyberspace. This work should be done and must be permanently updated. The task to define the base support documentation and to develop up-to-date mechanisms should be a follow-on work to this thesis.

6.5.4. Promulgation of Sectorial Doctrine

In the same base of was mentioned in the previous paragraph, and to fulfil what is demanded in the NIS Directive, it is necessary to define the doctrine to the Maritime Transport Sector. This must be done by the ISAC coordinator, together with the CNCS and in cooperation with the members of the ISAC and the DGRM.

The drafting of this doctrine could also be an academic work and would be crucial to give scientific support to the future sectorial doctrine.

Bibliography

[1] American Bureau of Shipping, The Application of Cybersecurity Principles to Marine and Offshore Operations Vol1 - Cybersecurity, vol. 1, Houston: American Bureau of Shipping, 2016.

[2] Lloyd's Register, Cyber-enabled ships, Southampton : Lloyd's Register, 2016.

[3] ENISA, Port Cybersecurity, Brussels: EU, 2019.

[4] Assembleia da Républica, Law n.º 46/2018, 13 August - Regime Juridico de Segurança do Ciberespaço, Lisbon: Diário da Républica, 2018.

[5] S. Crawford and L. Stucki, "Peer review and the changing research record," *J. Am. Soc. Sci.,* vol. 41, no. 3, pp. 222-228, 1990.

[6] H. R. Yarger, Strategic Theory for the 21st Century: The Little Book on Big Strategy, Carlisle: U.S. Army War College, 2006.

[7] A. Gonçalves, P. Sousa and M. Zacarias, "Using DEMO and activity theory to manage organization change," in *CENTERIS 2013 - Conference on ENTERprise Information Systems*, Lisbon, Portugal, 2013.

[8] L. S. Vygotsky, Mind in society: The development of higher psychological processes, Cambridge: Harvard University Press, 1978.

[9] A. Leontiev, Activity, Consciousness and Personality, N.J.: Prentice-Hall, 1978.

[10] I. T. Wangsa, L. Uden and S. F. Mills, "Using Activity Theory to Develop Requirements Analysis Framework for Collaborative Working Environments," in *15th International Conference on Computer Supported Cooperative Work in Design*, Laussane, Switzerland, 2011.

[11] T. Iyamu and I. Shaanika, "The use of activity theory to guide information systems research," *Education and Information Technologies,* pp. 165-180, 15 Jan 2015.

[12] Y. Engeström, “Expansive Learning at Work: toward an activity theoretical reconceptualization,” *Journal of Education and Work, Vol.14 Nº1,* 2001.

[13] A. Goncalves, A. Correia and L. Cavique, “Developing anti-bribery organization system based on quantitative pair-wise information an approach based on activity theory,” in *12th Iberian Conference on Information Systems and Technologies (CISTI)*, Lisbon, Portugal, 2017.

[14] Y. Engeström, “Expansive Visibilization of Work: An Activity Theoretical Perspective,” *Computer Supported Cooperative Work, vol.8,* pp. 63-93, 2000.

[15] Y. Engeström, Learning by expanding: an activity theoretical approach to developmental research, Helsinki: Orienta-Konsultit, 1987.

[16] D. Mwanza, Towards an Activity-Oriented Design Method for HCI Research and Practice, United Kingdom: The Open University, 202.

[17] B. Latour, Science in Action: How to Follow Scientists and Engineers Through Society, Cambridge: Harvard University Press, 1987.

[18] D. Cressman, Brief Overview of Actor-Network Theory: Punctualization, Heterogeneous Engineering & Translation, Burnaby: Simon Fraser University, 2009.

[19] B. Latour, “On Actor-Network Theory: A Few Clarifications,” *Soziale Welt,* vol. 47, no. 4, pp. 369-381, 1996.

[20] M. Callon, “Society in the Making: The Study of Technology as a Tool For Sociological Analysis,” in *The Social Construction of Technological Systems*, Cambridge, MIT Press, 1987, pp. 93-103.

[21] M. Callon, J. Law and A. Rip, Mapping the Dynamics of Science and Technology: Sociology of Science in the Real World, London: MacMillan Press, 1986.

[22] J. Law and M. Callon, “Engineering and Sociology in a Military Aircraft Project: A Network Analysis of Technological Change,” *Social Problems,* vol. 35, no. 3, pp. 284-297, 1988.

[23] M. Callon, “Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay,” *The Sociological Review,* vol. 1, no. 32, pp. 196-233, 1984.

[24] M. Callon, “Struggles and Negotiations to Define What is Problematic and What is Not,” in *The Social Process of Scientific Investigation. Sociology of the Sciences A Yearbook*, Dordrecht, D. Reidel Publishing Co., 1980, pp. 197-219.

[25] K. Foot, “Cultural-Historical Activity Theory as Practical Theory: Illuminating the Development of a Conflict Monitoring Network.,” *Communication Theory, Volume 11, Issue 1,* pp. 56-83, 10 Feb 2001.

[26] S. Carvalho, State of the Art - Annex to the Thesis "Assuring Cybersecurity on the Maritime Domain", Lisbon: IST, 2019.

[27] A. Tucci, “Dial C for Cyber Attack,” *Coast Guard Journal of Safety & Security at Sea, Proceedings of the Marine Safety & Security Council,* pp. 48-51, 07 2015.

[28] Conselho de Ministros, Estratégia Nacional de Segurança do Ciberespaço 2019-2023, Lisboa: Diário da República, 2019.

[29] R. Tsang, Cyberthreats, Vulnerabilities and Attacks on SCADA Networks, Berkeley: University of California, 2012.

[30] G. Schutze, “Safety4Sea,” 04 07 2018. [Online]. Available: https://safety4sea.com/cyber-threat-on-ships-what-is-true-what-is-vision-what-is-fantasy/. [Accessed 21 03 2019].

[31] C. D. Michel, P. F. Thomas and A. E. Tucci, Cyber Risks in the Marine Transportation System, Washington: US Coast Guard, 2017.

[32] M. Rouse, “Confidentiality, integrity, and availability (CIA triad),” WhatIs.com, 01 2015. [Online]. Available: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA. [Accessed 21 10 2018].

[33] USCG, Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities, Washington: USCG, 2017.

[34] IET Standards - Department for Transport, Code of Practice: Cyber Security for Ships, London: Her Majesty's Stationery Office, 2017.

[35] HM Goverment, “Ship Security Guidance,” 06 07 2018. [Online]. Available: https://www.gov.uk/guidance/maritime-security#ship-security-plans.

[36] IMO, The Guidelines on Cybersecurity on board Ships, New York: IMO, 2015.

[37] IMO, Guidance for the Development of national maritime security legislation, New York: IMO, 2016.

[38] ENISA, Analysis of cyber security aspects in the maritime sector, Brussels: EU, 2011.

[39] International Telecommunication Union (ITU), Global Cybersecurity Index (GCI) 2018, Geneve: ITU, 2018.

[40] C. Matis, “The Influence of Organizational Culture on Organizational Structures,” *Managerial Challenges of the Contemporary Society, vol. 7 no. 2,* pp. 179-184, 2014.

[41] F. Münch, “From Europe to North America to Asia: Overcoming the hurdles of Interdisciplinary Multicultural Teams through a design-driven process,” *Management international, 20(special),* pp. 38-48, 2016.

[42] United Nations, “Portugal,” 21 12 2018. [Online]. Available: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/136-Portugal.

[43] Conselho de Ministros, Law Decree 19/2013, 21 March - Conceito Estratégico de Defesa Nacional, Lisboa: Diário da Républica, 2013.

[44] Conselho de Ministros, Estratégia Nacional de Segurança do Ciberespaço, Lisbon: Diário da Républica, 2015.

[45] European Parliament ; European Council, Directive (EU) 2016/1148, Brussels: EU, 2016.

[46] Conselho de Ministros, Law Decree nº 69/2014, 9 May - GNS Alteração 2, Lisbon: Diário da Républica, 2014.

[47] Defense Minister, Decree n.º 13692/2013 - Orientação Política para a Ciberdefesa, Lisbon: Diário da Républica, 2013.

[48] CNCS, Quadro Nacional de Referência para a Cibersegurança, Lisboa: CNCS, 2019.

[49] CNCS, Roteiro para Capacidades Mínimas de Cibersegurança, Lisboa: CNCS, 2019.

[50] N. Lord, “What is the NIS Directive? Definition, Requirements, Penalties, Best Practices for Compliance, and More,” Digital Guardian, 12 09 2018. [Online]. Available: https://digitalguardian.com/blog/what-nis-directive-definition-requirements-penalties-best-practices-compliance-and-more. [Accessed 15 02 2019].

[51] Associação Portuguesa de Segurança, “Proteção Civil,” 09 01 2019. [Online]. Available: https://www.apsei.org.pt/areas-de-atuacao/protecao-civil/protecao-e-gestao-de-risco-de-infraestruturas-criticas/.

[52] Conselho de Ministros, Law Decree n.º 62/2011, 9 May - Infraestruturas Criticas, Lisbon: Diário da República, 2011.

[53] Conselho de Ministros, Law-decree n.º 43/2002, 2 of march - Sistema de Autoridade Maritima Nacional, Lisbon: Diário da República, 2002.

[54] Conselho de Ministros, Law-decree n.º 44/2002, 02 March - Autoridade Maritima Nacional, Lisbon: Diário da República, 2002.

[55] Conselho de Ministros, Law-decree n.º 248/95, 21 September - Organização da Polícia Marítima, Lisbon: Diário da República, 1995.

[56] Conselho de Ministros, Law-decree 226/2006, 15 November - Segurança Portuária, Lisbon: Diário da República, 2006.

[57] Conselho de Ministros, Law-decree 49-A/2012, 29 of February - Direcção-Geral de Recursos Naturais, Segurança e Serviços Marítimos, Lisbon: Diário da República 2012, 2012.

[58] DGRM, “Funções e Atribuições,” 10 11 2018. [Online]. Available: https://www.dgrm.mm.gov.pt/web/guest/dgrm-competencias-e-organica.

[59] AMT, “NATUREZA, MISSÃO E ÂMBITO,” AMT, 12 02 2015. [Online]. Available: http://www.amt-autoridade.pt/amt/natureza-miss%C3%A3o-e-%C3%A2mbito. [Accessed 8 12 2019].

[60] IET Standards - Department for Transport, Code of Practice: Cyber Security for Ports and Port Systems, London: Her Majesty's Stationery Office, 2016.

[61] K. Irion, “The Governance of Network and Information Security in the European Union: The European Public-Private Partnership for Resilience (EP3R),” in *The Secure Information Society*, London, Springer, 2013, pp. 83-116.

[62] European Commission High Representative of the European Union for Foreign Affairs and Security Policy, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels: European Commission, 2013.

[63] United Nations, “Business.un.org,” 2019. [Online]. Available: https://business.un.org/en/entities/13.

[64] W. Ashford, “NotPetya offers industry-wide lessons, says Maersk’s tech chief,” 7 6 2019. [Online]. Available: https://www.computerweekly.com/news/252464773/NotPetya-offers-industry-wide-lessons-says-Maersks-tech-chief. [Accessed 8 12 2019].

[65] J. S. Paulo, “Armada e Autoridade Marítima. Poupar o quê? Eficiente para quem?,” 15 01 2017. [Online]. Available: https://risco-continuo.blogs.sapo.pt/armada-e-autoridade-maritima-poupar-o-599801. [Accessed 8 12 2019].

[66] ENISA, EP3R 2010-2013 Four Years of Pan-European Public Private Cooperation, Brussels: European Union, 2014.

[67] M. Manley, “Cyberspace’s Dynamic Duo: Forging a Cybersecurity Public-Private Partnership,” *Journal of Strategic Security,* vol. 8, no. 3, pp. 85-98, 2015.

[68] K. K. Christensen and K. L. Petersen, “Public–private partnerships on cyber security: a practice of loyalty,” *International Affairs,* vol. 93, no. 6, p. 1435–1452, 2017.

[69] O. Bures, “Contributions of private businesses to the provision of security in the EU: beyond public-private partnerships,” *Crime Law Soc Change,* no. 67, p. 289–312, 2014.

[70] ENISA, Information Sharing and Analysis Centres (ISACs) - Cooperative models, Brussels: European Union Agency for Network and Information Security (ENISA), 2017.

[71] CNCS, ISAC Portugal, Lisboa: CNCS, 2019.

[72] B. Bender, “Cybersecurity & Maritime Domain,” EMSA, Lisbon, 2019.

[73] M. F. Triola, Introdução à Estatística, Rio de Janeiro: LCT, 1999.

[74] D. M. Levine, M. L. Berenson and D. Stephan, Estatística: Teoria e Aplicações usando Microsoft Excel em Português, Rio de Janeiro: LCT, 2000.

[75] L. J. Cronbach, “Coefficient Alpha and the internal structure of tests,” *Psychometrika,* no. 16, pp. 297-334, 1951.

[76] R. Peterson, “A Meta-Analysis of Cronbach's Coefficient Alpha,” *Journal of Consumer Research,* vol. 21, pp. 381-91, 02 1994.

[77] J. Maroco and T. Garcia-Marques, “Qual a fiabilidade do alfa de Cronbach? Questões antigas e soluções modernas?,” *Laboratório de Psicologia,* no. 4(1), pp. 65-90, 2006.

[78] P. Pernik, J. Wojtkowiak and A. Verschoor-Kirss, National Cyber Security Organisation: UNITED STATES, Tallinn: CCDCOE, 2016.

[79] B. Parker and G. Glay, “The Coast Guard and Cybersecurity - A legal framework for prevention and response,” *The Coast Guard Proceedings of the Maritime Safety & Security Council,* pp. 8-11, 2014.

[80] U.S. Department of Homeland Security, 2015 Transportation Systems Sector-Specific Plan, Washington: DHS, 2015.

[81] U.S. Department of Homeland Security, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, Washington: DHS, 2013.

[82] USCG, Reporting Suspicious Activity and Breaches of Security, Washington: DHS, 2016.

[83] USCG, Maritime Bulk Liquids Transfer, Offshore Operations, and Passenger Vessel Cybersecurity Framework Profile, Washington: USCG, 2017.

[84] USCG, Cyber Strategy, Washington: USCG, 2015.

[85] L. Brooks, “Coast Guard Captain of the Port,” *The Coast Guard Proceedings of the Maritime Safety & Security Council,* pp. 14-18, 2018.

[86] J. Couch and D. Campbell, “The Coast Guard’s Marine Transportation System Recovery Program,” *The Coast Guard Proceedings of the Maritime Safety & Security Council,* pp. 35-40, 2018.

[87] P. Brangetto, National Cyber Security Organisation in France, Tallin: NATO CCD COE, 2015.

[88] L. Ducamin and F. Charbonnier, Protection des infrastructures critiques: approches physique et cyber, Paris: SGDSN, 2017.

[89] Premier Ministre, Instruction Interministérielle - relatif à l'organisation et à la cootdination de la sûreté maritime et portuaire, Paris: SGDSN, 2018.

[90] DGITM, L'essentiel en sûreté portuaire, Paris: Ministère de l'Écologie, do Développement des Transports et du Logement, 2012.

[91] DGITM, Note techique du 25 février 2015 relative à la certification de sûreté d'un navire battant pavillon français, Paris: Ministère de l'Écologie, do Développement des Transports et du Logement, 2015.

[92] Gouvernement Français, Arrête du 23 novembre 1987 relatif à la sécurité des navires Reglement General, Paris : République Française, 1987.

[93] DGITM, Ports Maritimes - Code des Transports - Code des Ports Maritimes, Paris: Ministère de l'Écologie, do Développement des Transports et du Logement, 2017.

[94] Gouvernement Français, Code de la Défense, Paris: République Française, 2004.

[95] European Parliament ; European Council, UE RE 725 / 2004, Brussels: UE, 2004.

[96] IMO, International Ship and Port Facility and Security Code, New York: International Maritime Organization, 1998.

[97] A. Cendoya, National Cyber Security Organisation in Spain, Tallin: NATO CCD COE, 2016.

[98] Presidencia del Gobierno, “Estrategia de Seguridad Marítima Nacional 2013,” Gobierno de España, Madrid, 2013.

[99] Presidencia del Gobierno, “Estrategia de Ciberseguridad Nacional 2013,” Gobierno de España, Madrid, 2013.

[100] Presidencia del Gobierno, “Estrategia de Seguridad Nacional 2017,” Gobierno de España, Madrid, 2017.

[101] Gobierno de España, “Real Decreto 1008/2017 - Estrategia de Seguridad Nacional 2017,” in *Código de derecho de la ciberseguridad*, Madrid, Boletín Oficial del Estado Instituto Nacional de Ciberseguridad, 2017, pp. 31-61.

[102] Gobierno de España, “Orden TIN/3016/2011, de 28 de octobre,” in *Código de derecho de la ciberseguridad.*, Madrid, Boletín Oficial del Estado Instituto Nacional de Ciberseguridad, 2017, pp. 154-157.

[103] Gobierno de España, “Ley 36/2015, de 28 de septiembre, de Seguridad Nacional,” in *Código de derecho de la ciberseguridad*, Madrid, Boletín Oficial del Estado Instituto Nacional de Ciberseguridad, 2017, pp. 8-19.

[104] Gobierno de España, “Orden PRA/33/2018, de 22 de enero,” in *Código de Derecho de la Ciberseguridad*, Madrid, Boletín Oficial del Estado Instituto Nacional de Ciberseguridad, 2017, pp. 20-23.

[105] Gobierno de España, “Código de Derecho de la Ciberseguridad,” in *Orden PRA/116/2017, de 9 de febrero*, Madrid, Boletín Oficial del Estado Instituto Nacional de Ciberseguridad, 2017, pp. 26-30.

[106] Gobierno de España, “Real Decreto-ley 12/2018, de 7 de septiembre - Seguridad de las Redes y Sistemas de Información,” in *Código de Derecho de la Ciberseguridad*, Madrid, Boletín Oficial del Estado Instituto Nacional de Ciberseguridad, 2017, pp. 177-181.

[107] Gobierno de España, “Código de Derecho de la Ciberseguridad,” in *Ley 8/2011, de 28 de abril - Medidas para la Protección de las Infraestructuras Criticas*, Madrid, Boletín Oficial del Estado Instituto Nacional de Ciberseguridad, 2017, pp. 231-241.

[108] Gobierno de España, “Real Decreto 704/2011, de 20 de mayo - Reglamento de Protección de las Infraestructuras Críticas,” in *Código de Derecho de la Ciberseguridad*, Madrid, Boletín Oficial del Estado Instituto Nacional de Ciberseguridad, 2017, pp. 242-259.

[109] Gobierno de España, “Resolución de 8 de septiembre de 2015 - Contenidos Mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos,” in *Código de Derecho de la Ciberseguridad*, Madrid, Boletín Oficial del Estado Instituto Nacional de Ciberseguridad, 2017, pp. 260-279.

[110] Ministerio de Fomento, “Capitanías marítimas,” 11 10 2018. [Online]. Available: https://www.fomento.gob.es/marina-mercante/capitanias-maritimas/capitanias-maritimas-y-distritos-maritimos.

[111] Ministerio de Fomento, “Inspección marítima,” 10 11 2018. [Online]. Available: https://www.fomento.gob.es/marina-mercante/inspeccion-maritima.

[112] Ministerio de Fomento, “Normativa marítima y cooperación internacional,” 10 11 2018. [Online]. Available: https://www.fomento.gob.es/marina-mercante/normativa-maritima-y-cooperacion-internacional/subdireccion-general-de-normativa-maritima-y-cooperacion-internacional.

[113] Ministerio de Fomento, “Dirección General de la Marina Mercante,” 10 11 2018. [Online]. Available: https://www.fomento.gob.es/el-ministerio/organizacion-y-funciones/secretaria-de-estado-de-infraestructuras-transportes-y-vivienda/secretaria-general-de-transporte/direccion-general-de-la-marina-mercante.

[114] A. M. Osula, National Cyber Security Organisation: United Kingdom, Tallinn: CCDCOE, 2015.

[115] HM Goverment, The UK National Strategy for Maritime Security, London: Her Majesty's Stationery Office, 2014.

[116] HM Goverment, National Security Strategy and Strategic Defence and Security Review 2015, London: Her Majesty's Stationery Office, 2015.

[117] National Cyber Security Centre, “Cyber Incidents,” 01 08 2016. [Online]. Available: https://www.ncsc.gov.uk/scheme/cyber-incidents.

[118] National Cyber Security Centre, “National Cyber Security Centre,” 04 09 2018. [Online]. Available: https://www.ncsc.gov.uk/information/crest-cyber-security-incident-response-csir-scheme.

[119] HM Goverment, “Maritime and Coastguard Agency,” 23 11 2018. [Online]. Available: https://www.gov.uk/government/organisations/maritime-and-coastguard-agency/about.

[120] S. A. Shaikh, Future of the Sea: Cyber Security, London: Goverment Office for Science, 2017.

[121] Department of Transports, Port Security Regulations 2009, London: Her Majesty's Stationery Office, 2009.

[122] DGRM, “Proteção dos Navios e das Instalações Portuárias (ISPS),” 10 11 2018. [Online]. Available: https://www.dgrm.mm.gov.pt/web/guest/am-cp-protecao-das-instalacoes-portuarias-e-dos-portos.

[123] DGRM, “Navios,” 11 10 2018. [Online]. Available: https://www.dgrm.mm.gov.pt/web/guest/am-ce-navios.

[124] European Parliament ; European Council, Directive (EU) 2008/114/CE, Brussels: EU, 2008.

[125] European Parliament ; European Council, Directive (EU) 2005/65/CE, Brussels: EU, 2005.

[126] Conselho de Ministros, Law Decree nº 136/2017, 6 november - GNS Alteração 3, Lisbon: Diário da Républica, 2017.

[127] United Nations, “UN e-Government Knowledgebase,” 18 01 2019. [Online]. Available: https://publicadministration.un.org/egovkb/en-us/.

[128] J. R. Lincoln, J. Olson and M. Hanada, “Cultural Effects on Organizational Structure: The Case of Japanese Firms in the United States,” *American Sociological Review Vol.43 Issue 6,* pp. 829-847, Dec 78.

[129] D. K. Allen, A. Brown, S. Karanasios and A. Norman, “How Should Technology-Mediated Organizational Change Be Explained? A Comparison of the Contributions of Critical Realism and Activity Theory,” *MIS Quarterly, Vol. 37 Issue 3,* pp. 835-854, Sep 2013.

[130] Y. Engeström, R. Miettinen and R.-L. Punamäki, Perspectives on activity theory, Cambridge : Cambridge University Press, 1999.

[131] Y. Engeström, The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility, Human-Computer Interaction, 2000.

[132] Gobierno de España, REAL DECRETO 1617/2007, de 7 de diciembre - la protección de los puertos y del transporte marítimo, Madrid: Boletín Oficial del Estado, 2007.

[133] Critical National Infrastructures, “Critical National Infrastructure,” 23 11 2018. [Online]. Available: https://www.cpni.gov.uk/critical-national-infrastructure-0.

[134] ENISA, Information Sharing and Analysis Centres (ISACs) - Cooperative models, Brussels: European Union Agency for Network and Information Security (ENISA), 2017.

[135] President of United States, National Cyber Strategy of the United States of America, Washington: The White House, 2018.

[136] President of the United States, National Security Strategy of the United States, Washington: The White House, 2017.

[137] President of the United States, Presidential Decision Directive/NSC-63. Critical Infrastructure Protection, Washington: The White House, 1998.

[138] President of the United States, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, Washington: The White House, 2009.

[139] U.S. Department of Homeland Security, Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection, Washington: DHS, 2003.

[140] U.S. Department of Homeland Security, National Infrastructure Protection Plan 2013, Washington: DHS, 2013.

[141] U.S. Department of Homeland Security, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, Washington: DHS, 2013.

[142] U.S. Department of Homeland Security, Transportation Systems Sector-Specific Plan – 2015, Washington: DHS, 2015.

[143] U.S. Congress, Maritime Transportation Security Act of 2002, Washington: U.S. Congress, 2002.

[144] U.S. Congress, Ports and Waterways Safety Act of 1972, Washington: U.S. Congress, 1972.

[145] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Washington: NIST, 2018.

[146] President of the United States, Executive Order -- Improving Critical Infrastructure Cybersecurity, Washington: The White House, 2013.

[147] National Institute of Standards and Technology , Guide to Industrial Control Systems (ICS) Security, Washington: NIST, 2015.

[148] USCG, “United States Coast Guard Organization Chart,” USCG, 26 07 2018. [Online]. Available: https://www.uscg.mil/Units/Organization/#cg6. [Accessed 25 11 2018].

[149] USCG, “Domestic Ports Division,” USCG, 12 02 2018. [Online]. Available: https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/fac1/. [Accessed 21 11 2018].

[150] USCG, “Office of Port & Facility Compliance,” USCG, 15 05 2018. [Online]. Available: https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/cgfac/. [Accessed 22 11 2018].

[151] I. M. Fund, France Selected Issues Paper, IMF Country Report, No. 13/252, Washington: IMF, 2013.

[152] European Union, EU Digital Agenda Scoreboard for France: EU Digital Agenda,, Brussels: EU, 2013.

[153] Commissariat général à l'investissement, Programme d'investissements d'avenir – situation et perspectives, Paris: CGI, 2014.

[154] J.-C. Mallet, Défense et Sécurité nationale: le Livre blanc, Paris: Defense Francaise, 2008.

[155] Agence Nationale de la Sécurité des Systèmes d'Information, Défense et sécurité des systèmes d'information. Stratégie de la France, Paris: ANSSI, 2011.

[156] Gouvernement Français, La nouvelle France industrielle. Présentation des feuilles de route des 34 plans de la nouvelle France industrielle, Paris: République Française, 2014.

[157] Gouverment Français, French White Paper on National Defence and Security, Paris: République Française, 2013.

[158] Gouverment Français, LOI n° 2013-1168 du 18 décembre 2013 Programmation militaire pour les années 2014 à 2019, Paris: République Française, 2014.

[159] Agence Nationale de la Sécurité des Systèmes d'Information, CERT-FR. Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, Paris: République Française, 2019.

[160] Legifrance.gouv.fr, Arrêté du 2 juin 2006 modifié fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordon-nateurs desdits secteurs, Paris: Journal officiel de la République française, 2006.

[161] Gouverment Français, Objectifs de cybersécurité', Paris: Secré-tariat général de la défense et de la sécurité nationale, Paris: République Française, 2014.

[162] Shipping Virtual Services, "IACS Publishes Cyber Safety Recommendations," Shipping Virtual Services, 2 10 2018. [Online]. Available: https://shipip.com/new/iacs-publishes-cyber-safety-recommendations/. [Accessed 21 12 2018].

[163] H. R. Yarger, "Strategic Theory for the 21st Centu," My Essay Papers, 02 2006. [Online]. Available: http://helpessay.myessaypaper.co/strategic-theory-for-the-21st-centu.html. [Accessed 10 12 2018].

[164] J. F. S. Jr., Federal Research and Development Funding: FY2013, Washington: Congressional Research Service, 2013.

[165] D. G. Bonett and T. A. Wright, "Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning," *Journal of Organizational Behavior,* 29 08 2014.

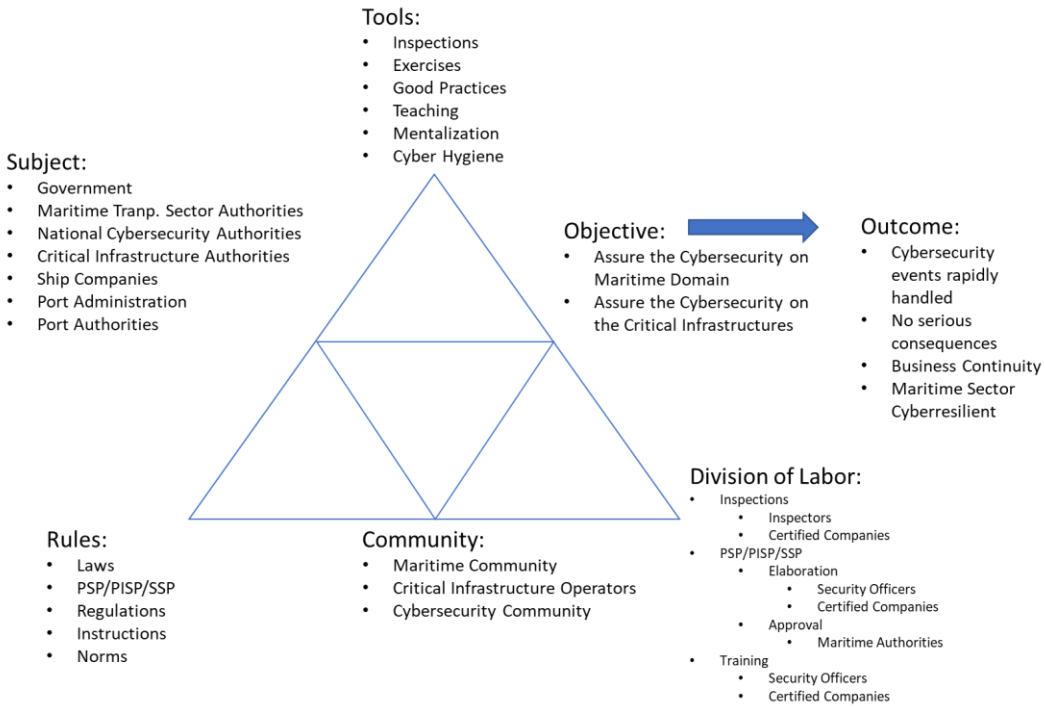
Appendix 1

Applying the Proposed Analysis Model

Developing the analysis model, we concluded that the established model to investigate the problem and justify the proposed solution is based on the Grand Strategy and the Activity Theory, and the problem can be easily framed on both these two theories:

Gran Strategy [4]	Activity Theory [17]
Ends **Explain "what" is to be accomplished**	Objective Why is the activity taking place?
	Outcome What is the desired Outcome from carrying out this activity?
Ways **Answer the big question of "how" the objectives are to be accomplished**	Rules Are there any cultural norms, rules or regulations governing the performance of this activity?
	Division of Labor Who is responsible for what, when carrying out this activity, and how are the roles organised?
	Community What is the environment in which this activity is carried out?
Means **Set the boundaries for the types and levels of support modalities that will be made available**	Tools By what means are the subjects performing this activity?
	Subjects Who is involved in carrying out this activity?

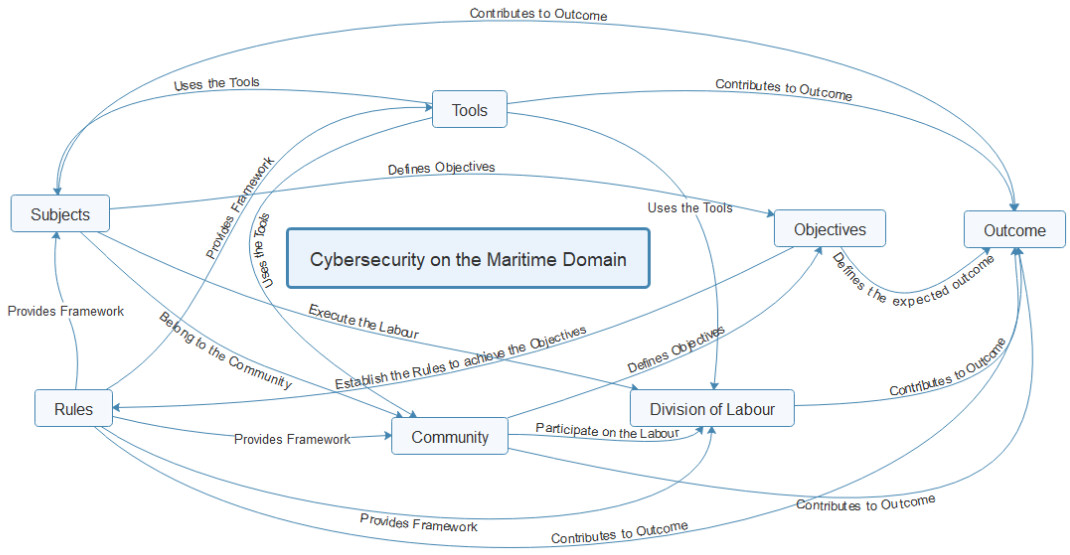
Also, in a first generic approach for the TA will be the following:



The relationship between Grand Strategy, AT and ANT could be summarised like this:

Grand Strategy	TA	ANT	
		Mediators	Intermediates
Ends	Objectives Outcome	Objectives	Outcome
Ways	Rules Division of Labour Community	Rules Division of Labour	Community
Means	Tools Subjects	Tools	Subjects

In this first level of ANT, we can schematize in the following way:



Applying this model to the “State of the Art” of the chosen countries resulted in the following schemes.

United States

Activity Theory Analysis

Objective Why is the activity taking place?	Outcome: What is the desired Outcome from carrying out this activity?	Subjects: Who is involved in carrying out this activity?	Tools: By what means are the subjects performing this activity?
• Assure the cybersecurity on the Maritime Domain; • Assure the Resilience of the Maritime Domain; • Assure the rapid response to a cybersecurity event on the Maritime Domain; • Simultaneously, assure the cybersecurity of the critical Maritime Transport Sector (CI).	• The Maritime Domain is Cyber resilient; • The Maritime Domain Community has cyber hygiene knowledge and behaviours; • All cyber events on the Maritime Domain are rapidly responded and analysed; • Lessons learned are taken from the events and implements in new best practices or norms; • The Maritime Domain actors have SSP / FSP implemented and validated; • C4All the Maritime Domain actors know their role in the maritime cybersecurity organisation; • The Maritime Transport Critical Sector are cyber protected	• Department of Homeland Security (DHS); • United States Coast Guard (USCG); • Captain of the Port (COTP • USCG Office of Port and Facility Compliance • Area Maritime Security Committees (AMSCs) • Local Port Authorities; • Company Security Officers and Port Security Officers; • Officer in Charge Maritime Inspections; • Domestic Ports Division; • Office of Port & Facility Compliance; • Office of Cyberspace Forces;	• National Infrastructure Protection Plan (NIPP) - CI protection; • Cyber Governance and Cyber Risk Management Program Implementation Guidance; • USCG "Cyber Strategy" • Inspections, exercises and patrols to the vessels and facilities; • Area Maritime Security Plan (AMSP); • Port-Wide Cybersecurity Risk Assessment Tools and Methodologies; • Cybersecurity Information Sharing; • Incorporate Cybersecurity into Training and Education; • CERTs; • CSIRTs; • SOCs;

Rules: Are there any cultural norms, rules or regulations governing the performance of this activity?	Community: What is the environment in which this activity is carried out?	Division of Labour: Who is responsible for what, when carrying out this activity, and how are the roles organised?
Maritime Transportation Security Act (MTSA) - physical and personnel security standards for ports, facilities, and vessels Magnuson Act - authorises the president to "safeguard against the destruction, loss, or injury from sabotage or other subversive acts," and from accidents to "vessels, harbours, ports, and waterfront facilities." Ports and Waterways Safety Act of 1972 (PWSA): to protect ports, waterways, maritime facilities, and vessels from incidents involving negligence or sabotage. Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity Maritime Bulk Liquids Transfer, Offshore Operations, and Passenger Vessel Cybersecurity Framework Profiles' Guidelines for Addressing Cyber Risks at the Maritime Transportation Security Act (MTSA) Regulated Facilities	Maritime Transport Industry; Harbour Masters; Navigation Companies; Harbour Operators; Maritime Community; Critical Infrastructure Owners and Operators; Maritime Off structures Owners and Operators; Local Port Authorities; Ship-owners, operators and handlers. Maritime Authorities Cybersecurity Community Cybersecurity Organisms	USCG: • (sector-specific agency) - primary responsibility for the safety, security, managing the responses to incidents impacting the Federal navigable waters and ports and coordinating and expediting the recovery of the maritime transportation system • Office of Cyberspace Forces - Responsible to USCG obtain Cyberspace capabilities, competencies, and capacity to meet operational requirements; • Office of Port & Facility Compliance - provide clear and timely regulations, policy and direction to USCG Commanders and other maritime stakeholders; • Domestic Ports Division - develop and implement programs to prevent safety, security, and environmental incidents in the maritime arena; • Officer in Charge Maritime Inspections (OCMI) and local Port Authorities - inspections, exercises and patrols to the vessels and facilities; Captain of the Port - enforce within their respective areas port safety and security regulations; Company Security Officers and Port Security Officers: • Facility Security Assessment; • Facility Security Plan.

Other Variable Analysis

CGI Rank	**2**
E-Government Rank	11
Is maritime transport a CI?	Yes, inside on one of the 16 critical sectors - transportation
Specific Cybersecurity Organism?	Yes, under the Department of Homeland Security > National Protection and Programs Directorate > Office of Cybersecurity and Communications
Specific Cybersecurity Organism for Maritime Domain?	No, the Cybersecurity on Maritime Domain is under the responsibility of USCG, like all the other aspects of Maritime security.
Specific Rules Law for Cybersecurity in the MD?	Yes, issued by the USCG in cooperation with NIST and Industry
The Security Laws were adopted to Include Cybersecurity in the MD?	Yes, or reinterpret to encompass the cybersecurity aspect.
Was it adopted a new organisation to cope cybersecurity in MD?	No, it was used the already implemented for maritime security.
The PSP, PFSO and PSP encompasses cybersecurity	Yes, it is mandatory through the implementation of the Executive Order (EO) 13636 and other specific regulations by the USCG
Specific Organisation to respond to a Cybersecurity event in the MD?	Yes, by the national cyber event reaction but with specific tasks to the USCG.

France

Activity Theory Analysis

Objective Why is the activity taking place?	Outcome: What is the desired Outcome from carrying out this activity?	Subjects: Who is involved in carrying out this activity?	Tools: By what means are the subjects performing this activity?
Assure the cybersecurity on the Maritime Domain; Assure the Resilience of the Maritime Domain; Assure the rapid response to a cybersecurity event on the Maritime Domain; Simultaneously, assure the cybersecurity of the critical Maritime Transport Sector (CI).	The Maritime Domain is Cyber resilient; The Maritime Domain Community has cyber hygiene knowledge and behaviours; All cyber events on the Maritime Domain are rapidly responded and analysed; Lessons learned are taken from the events and implements in new best practices or norms; The Maritime Domain actors have SSP / FSP implemented and validated; C4All the Maritime Domain actors know their role in the maritime cybersecurity organisation; The Maritime Transport Critical Sector are cyber protected.	Prime Minister Minister of the La transition Écologique et Solidaire Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) National Network and Information Security Agency (ANSSI) Commission interministérielle de sûreté maritime et portuaire (CISMaP) Operational Centre for the Security of Information Systems Operators of Critical Importance Comité interministériel de la mer (CIMer) Direction Générale des Infrastructures des Transports et de la Mer (DGITM) Groupe Interministériel se Sûreté du Transport Maritime (GISTMOP) Comités Locaux de Sûreté Portuaire (CLSP) Commission Centrale de Sécurité (CCS) Direction des Affaires Maritimes (DAM) Direction des Services de Transport (DST) Préfet de zone Préfet de département Préfet Maritime Harbour Master Harbour Security Agent Harbour Manager École Nationale Supérieure Maritime Centres de Sécurité des Navires (CNS) Organismes de Sûreté Habilités (OSH) Ship-owner Ship operator Ship handler Company Security Officer (CSO) Port Authority Port Facility Explorer	Plan Vigipirate Plan Pirate-Mer Diffusion of a good practice's guide/flyer; Imposition of the IMO directives Mandatory Formation for Key Roles Mandatory cyber hygiene formation Mandatory schedule of exercises Inspections Cybersecurity Information Sharing; Incorporate Cybersecurity into Training and Education; CERTs CSIRTs SOCs

Rules: Are there any cultural norms, rules or regulations governing the performance of this activity?	Community: What is the environment in which this activity is carried out?	**Division** of Labour: Who is responsible for what, when carrying out this activity and how are the roles organised?
Directive Nationale de Sécurité - For each CI Sector Plan de Sécurité d'Opérateur (PSO) d'Importance Vitale - For each CI operator Plan Particulier de Protection (PPP) Plan de protection externe- For each CI "Dispositif de Sécurité des activités d'importance vitale"(SAIV) - security plans for the critical infrastructure includes physical and cyber considerations Plan de Sûreté du Port – PSP Plan de Sûreté de L'Installation Portuaire – PSIP ISPS (International Ship and Port Facility Security) (IMO 1998), EU Directive 2008/114/CE - Critical Infrastructures EU Regulations EU Regulation n. º 725/2004 - transposition of the SOLAS Convention, the ISPS Code EU Directive 2005/65/EU. -Enhancing port-security Directive (EU) 2016/1148 of 6 July 2016 - NIS directive IMO MSC-FAL.1-Circ.3 - Guidelines on Maritime Cyber Risk Management MSC—96/WP.9 - Measures to Enhance Maritime Security FAL 40/INF.4 - Guidelines on the Facilitation Aspects of Protecting the Maritime Transport Network from Cyber threats. Code des Ports Maritimes	Maritime Transport Industry; Harbour Masters; Navigation Companies; Harbour Operators; Maritime Community; Critical Infrastructure Owners and Operators; Maritime Off structures Owners and Operators; Local Port Authorities; Ship-owners, operators and handlers. Maritime Authorities Cybersecurity Community Cybersecurity Organisms	Minister of the "La transition Écologique et Solidaire" - approves the Directive Nationale de Sécurité for the transport sector Préfet de zone - Approves the Plan de Sécurité d'Opérateur Préfet Maritime • Approves the Plan Particular de Protection and the Plan de protection external for maritime CI. • Enforces the measures within his prerogatives called by the Vigipirate plan Préfet Département • It approves the Plan Particular de Protection and the Plan de protection external for land CI (Ports). • In charge of local implementation of the port security measures CIMer - establish the govern orientations for the maritime activities CISMaP - coordinates the security actions in the maritime domain between ministries ANSSI - issue the cybersecurity rules that must be fulfilled by the "Opérateur d'Importance Vitale" (OIV) DGITM - responsible for preparing and implementing the state politics concerning the transports and issuing the technical norms for the security of the infrastructures CLSP - Advises the Préfet Département concerning the port security, approves the risk evaluation of the ports and ports facilities, and their PSP and PSIP. DAM • elaboration and application of the security rules for the merchant ships • organise and conduct de ships inspections through CNS • planning and prevention of cybersecurity for the maritime sector in collaboration with the ANSSI • approves the SSP DST - elaborate and implement of the orientations to the transports policies for the maritime transports and elaborates and implements the politics for the harbours and maritime transports safety and security. OSH - private companies certified to execute security verifications to the maritime facilities and ships and verify that they comply with the approved security plan, conduct security exercises and give formation concerning this subject Ship-owner, operator and the ship handler - elaborate and submit to approval the SSP through the CSO Port Authority - Elaborates the PSP Port Facility Explorer - Elaborates the PSIP

Other Variable Analysis

CGI Rank	**8**
E-Government Rank	9
Is maritime transport a CI?	Yes, inside on one of the 12 critical sectors - transportation
Specific Cybersecurity Organism?	National Network and Information Security Agency (ANSSI)
Specific Cybersecurity Organism for Maritime Domain?	No, the Cybersecurity on Maritime Domain is under the responsibility of several state entities, the same that also have the obligation of the Maritime Security.
Specific Rules Law for Cybersecurity in the MD?	Yes, Article 130.39 of the "Arrête du 23 novembre 1987 relatif à la sécurité des navires Règlement General" They also state that in the technical note of the DGITM that cybersecurity is a requirement due to the UE RE 725/2004 that states, concerning the security of vessels and maritime facilities, interpreting that the paragraph B 8.3 to the B 8.10 of the ISPS encompasses cybersecurity.
The Security Laws were adopted to Include Cybersecurity in the MD?	Yes, or reinterpret to encompass the cybersecurity aspect.
Was it adopted a new organisation to cope cybersecurity in MD?	No, it was used the already implemented for maritime security.
The PSP, PFSO and PSP encompasses cybersecurity	Yes, is a mandatory area in the PSO and PP by the imposition of the ANSSI and DAM
Specific Organisation to respond to a Cybersecurity event in the MD?	Yes, by the national cyber event reaction but with specific tasks of the maritime authorities

Spain

Activity Theory Analysis

Objective Why is the activity taking place?	Outcome: What is the desired Outcome from carrying out this activity?	Subjects: Who is involved in carrying out this activity?	Tools: By what means are the subjects performing this activity?
Assure the cybersecurity on the Maritime Domain; Assure the Resilience of the Maritime Domain; Assure the rapid response to a cybersecurity event on the Maritime Domain; Simultaneously, assure the cybersecurity of the critical Maritime Transport Sector (CI).	The Maritime Domain is Cyber resilient; The Maritime Domain Community has cyber hygiene knowledge and behaviours; All cyber events on the Maritime Domain are rapidly responded and analysed; Lessons learned are taken from the events and implements in new best practices or norms; The Maritime Domain actors have SSP / FSP implemented and validated; C4All the Maritime Domain actors know their role in the maritime cybersecurity organisation; The Maritime Transport Critical Sector are cyber protected.	Prime Minister Consejo de Seguridad Nacional (CSN) Situation Centre of the National Security Department (DSN) Consejo Nacional de Ciberseguridad (CNC) Comité Especializado de Situación (CES) Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) Ministerio del Interior Comisión Nacional para la Protección de las Infraestructuras Críticas (CoNPIC) Critical operators Ministerio de Fomento Maritimes Captains Subdirección General de Seguridad, Contaminación e Inspección Marítima (SGSCIM) Dirección General de la Marina Mercante (DGMM) Recognised organisations of protection Company Official for the Maritime Protection Port Security Officer Harbour protection authority Advisory Committee for the Port Protection Interior and the Development Ministry Centro Criptológico Nacional (CCN) Centro de Respuesta a Incidentes de Seguridad de la Información (CERTSI).	Protection System of the Critical Infrastructures Mandatory Formation for Key Roles Mandatory cyber hygiene formation Mandatory schedule of exercises Inspections Cybersecurity Information Sharing; Incorporate Cybersecurity into Training and Education; CERTs CSIRTs SOCs

Rules: Are there any cultural norms, rules or regulations governing the performance of this activity?	Community: What is the environment in which this activity is carried out?	**Division** of Labour: Who is responsible for what, when carrying out this activity and how are the roles organised?
EU Directive 2008/114/CE - Critical Infrastructures EU Regulations EU Regulation n. º 725/2004 - transposition of the SOLAS Convention, the ISPS Code EU Directive 2005/65/EU. -Enhancing port-security Directive (EU) 2016/1148 of 6 July 2016 - NIS directive IMO MSC-FAL.1-Circ.3 - Guidelines on Maritime Cyber Risk Management MSC—96/WP.9 - Measures to Enhance Maritime Security FAL 40/INF.4 - Guidelines on the Facilitation Aspects of Protecting the Maritime Transport Network from Cyber threats. Royal Law 8/2011 Royal Decree 704/2011 CI Security Plans CI Specific Protection Plans Strategic Sectorial Plans Royal Law 1617/2007 of 7 December ISPS (International Ship and Port Facility Security) (IMO 1998) SOLAS convention (IMO 1974) Ship Security Plan (SSP) Ship Security Assessment (SSA) Port Facility Security Plan (PFSP) Port Security Plan (PSP) Port Facility Security Assessment (PFSA) Port Security Assessment (PSA)	Maritime Transport Industry; Harbour Masters; Navigation Companies; Harbour Operators; Maritime Community; Critical Infrastructure Owners and Operators; Maritime Off structures Owners and Operators; Local Port Authorities; Ship-owners, operators and handlers. Maritime Authorities Cybersecurity Community Cybersecurity Organisms	Prime minister - leads the CSN CSN - the management, leadership and promotion of the national security policy CNC - supports the CSN in assisting the Prime Minister on cybersecurity issues CES - helps the CSN in crises on cybersecurity matters Ministerio del Interior - Approves the Security Plans and the Specific Protection Plans under the proposition of the CNPIC CoNPIC - approves the Strategic Sectorial Plans Critical operators - responsible for the elaboration of the Operator's Protection Plan, Specific Protection Plan and collaborate in the formulation of the Strategic Sectorial Plans Ministerio do Fomento - responsible for the security of the maritime transport sector Maritimes Captains - are responsible for conducting the organisation control and direction of the security inspections of the Spanish merchant ships. SGSCIM o order and execute security inspections on the Spanish flagged vessels and other foreign ships under international agreements coverage o approves and verifies the implementation of the SSP o authorises the recognised organisations of protection Company Official for the Maritime Protection - conduct the protection evaluation and to elaborate the SSP Harbour protection authority - approves the assessment of the port facilities protection and approves the PFSP Recognised organisations of protection - private companies, certified to execute security verifications to the maritime facilities and ships and verify that they comply with the approved security plan, conduct security exercises and give formation concerning this subject Advisory Committee for the Port Protection - perform information concerning the evaluation of the harbour protection plan, previously his approval Interior and the Development Ministry - approves the PSP and establish an inspection system. Port Security Officer - Conduct Exercises, implement the Security Plan, coordination of security activities

Other Variable Analysis

CGI Rank	**19**
E-Government Rank	17
Is maritime transport a CI?	Yes, inside on one of the 12 critical sectors - transportation
Specific Cybersecurity Organism?	Centro Criptológico Nacional (CCN)
Specific Cybersecurity Organism for Maritime Domain?	No, the Cybersecurity on Maritime Domain is under the responsibility of several state entities, the same that also have the responsibility of the Maritime Security.
Specific Rules Law for Cybersecurity in the MD?	Yes, Ports and the harbour facilities are regulated by the Law 1617/2007 of 7 December, combined with the full compliance with critical infrastructures legislation
The Security Laws were adopted to Include Cybersecurity in the MD?	Yes, or reinterpret to encompass the cybersecurity aspect.
Was it adopted a new organisation to cope cybersecurity in MD?	No, it was used the already implemented for maritime security.
The PSP, PFSO and PSP encompasses cybersecurity	Yes, is a mandatory area in the SSP, PFSP and PSP by the imposition by the minimum contents defined by the State Security Secretariat, of the Interior Ministry
Specific Organisation to respond to a Cybersecurity event in the MD?	Yes, by the national cyber event reaction but with specific tasks of the maritime authorities

United Kingdom

Activity Theory Analysis

Objective Why is the activity taking place?	Outcome: What is the desired Outcome from carrying out this activity?	Subjects: Who is involved in carrying out this activity?	Tools: By what means are the subjects performing this activity?
Assure the cybersecurity on the Maritime Domain; Assure the Resilience of the Maritime Domain; Assure the rapid response to a cybersecurity event on the Maritime Domain; Simultaneously, assure the cybersecurity of the critical Maritime Transport Sector (CI).	The Maritime Domain is Cyber resilient; The Maritime Domain Community has cyber hygiene knowledge and behaviours; All cyber events on the Maritime Domain are rapidly responded and analysed; Lessons learned are taken from the events and implements in new best practices or norms; The Maritime Domain actors have SSP / FSP implemented and validated; C4All the Maritime Domain actors know their role in the maritime cybersecurity organisation; The Maritime Transport Critical Sector are cyber protected.	Prime Minister Government Communications Headquarters (GCHQ) Office of Cyber Security & Information Assurance (OCSIA) National Security Secretariat (NCS) Cyber Security Operations Centre (CSOC) National Technical Authority for Information Assurance (CESG) Lead Government Department (LGD) Centre for the Protection of National Infrastructure (CPNI) Department for Transport (DfT) Maritime and Coastguard Agency (MCA) National Maritime Security Committee (Industry) - NMSC(I) Maritime Security and Safety Management Branch - MSSMB Ship security officer (SSO) Cybersecurity officer (CySO) Port Security Committee (PSC) Port Security Authority (PSA) Recognised security organisations Company security officer (CSO) Port facility security officer (PFSO) Port Security Officer (PSO)	Mandatory Formation for Key Roles Mandatory cyber hygiene formation Mandatory schedule of exercises Inspections Cybersecurity Information Sharing; Incorporate Cybersecurity into Training and Education; CERTs CSIRTs SOCs

Rules: Are there any cultural norms, rules or regulations governing the performance of this activity?	Community: What is the environment in which this activity is carried out?	**Division** of Labour: Who is responsible for what, when carrying out this activity and how are the roles organised?
EU Directive 2008/114/CE - Critical Infrastructures EU Regulations EU Regulation n. º 725/2004 - transposition of the SOLAS Convention, the ISPS Code EU Directive 2005/65/EU. -Enhancing port-security Directive (EU) 2016/1148 of 6 July 2016 - NIS directive IMO MSC-FAL.1-Circ.3 - Guidelines on Maritime Cyber Risk Management MSC—96/WP.9 - Measures to Enhance Maritime Security FAL 40/INF.4 - Guidelines on the Facilitation Aspects of Protecting the Maritime Transport Network from Cyber threats. ISPS (International Ship and Port Facility Security) (IMO 1998) SOLAS convention (IMO 1974) National Strategy for Maritime Security (NSMS) Cyber Security Plan (CSP) Ship Security Plan (SSP) Ship Security Assessment (SSA) Port Facility Security Plan (PFSP) Port Security Plan (PSP) Port Facility Security Assessment (PFSA) Port Security Assessment (PSA) Cyber Security Assessment (CSA) IET Standards: Code of Practice - Cyber Security for Ships Code of Practice - Cyber Security for ports and Ports Systems	Maritime Transport Industry; Harbour Masters; Navigation Companies; Harbour Operators; Maritime Community; Critical Infrastructure Owners and Operators; Maritime Off structures Owners and Operators; Local Port Authorities; Ship-owners, operators and handlers. Maritime Authorities Cybersecurity Community Cybersecurity Organisms	OCSIA - provides strategic direction and coordinates action relating to cybersecurity and information assurance in the UK GCHQ -an offering or hosting strategic analyses of the threats, operational CS capabilities and cyber incident management. NCS - responsible for coordination on security and intelligence issues of strategic importance across government, including cybersecurity CSOC - monitor and coordinate incident response and share with businesses and the public information and advice on attacks against UK networks and users. CESG - Information Assurance arm and is running the CERT-UK LGD - responsible for the sector, and ensuring protective security is in place for critical assets CPNI - provides advice and assistance to those who have responsibility for protecting the CI from national security threats. (works with the operators of critical maritime infrastructure) DfT o regulates port and ship security o review and approves the security required from industry partners (PFSP, PSP, SSP) o undertakes the security assessments of ports/port facilities MCA o Assures the security compliance of the ships. o Conducts ships inspections NMSC (I) - the interaction between the commercial maritime industry and Government on maritime security matters. MSSMB - coordinates measures to ensure security in the maritime community, providing technical advice and guidance CSO - make the SSA, the SSP and submit them for approval. SSO - Implement the SSP, coordinate exercises and formations PSC and PSA o development and implementation of security policies, processes and procedures o make the SSA, CSA, PFSA, PSA, PFSP and PSP and submit them for approval o recognised security organisations - Can conduct the port and ships inspections PFSO - Implement the PFSP, coordinate exercises and education PSO - Implement the PSP, coordinate exercises and education CySO - The person or persons tasked to manage and coordinate the cybersecurity of a ship

Other Variable Analysis

CGI Rank	**19**
E-Government Rank	17
Is maritime transport a CI?	Yes, inside on one of the 13 critical sectors - transportation
Specific Cybersecurity Organism?	Office of Cyber Security & Information Assurance (OCSIA)
Specific Cybersecurity Organism for Maritime Domain?	No, the Cybersecurity on Maritime Domain is under the responsibility of several state entities, the same that also have the responsibility of the Maritime Security.
Specific Rules Law for Cybersecurity in the MD?	UK interprets that the relationship of the CSP to the SSP that are required by the UK and European legislation and the ISPS Code, through the Part B of the ISPS Code, paragraphs 8.1 to 8.10, that provide guidance on aspects to be included in the SSA, these include: radio and telecommunication systems (including computer systems and networks)
The Security Laws were adopted to Include Cybersecurity in the MD?	Yes, or reinterpret to encompass the cybersecurity aspect.
Was it adopted a new organisation to cope cybersecurity in MD?	No, it was used the already implemented for maritime security.
The PSP, PFSO and PSP encompasses cybersecurity	Yes, is a mandatory area in the SSP, PFSP and PSP by the imposition by the minimum contents defined by the Standards of the DfT
Specific Organisation to respond to a Cybersecurity event in the MD?	Yes, by the national cyber event reaction but with specific tasks of the maritime authorities

Appendix 2

Questionnaire and the Results

In this appendix, you can find the questions done in the survey and the results for each item.

What is your age?

	Community	Authorities	Academia	Total
Average	43,8	48,2	53,3	44,7

What is your gender?

	Community		Authorities		Academia		Total	
Male	236	75,64%	69	98,57%	4	100,00%	309	80,05%
Female	76	24,36%	1	1,43%	0	0,00%	77	19,95%
Total	312		70		4		386	
Mean	1,24		1,01		1,00			
Standard Dev.	0,43		0,12		0,00			
Variance	0,18		0,01		0,00			

What is your highest qualification?

	Community		Authorities		Academia		Total	
High Schools	6	1,93%	0	0,00%	1	25,00%	7	1,82%
Professional	11	3,54%	0	0,00%	0	0,00%	11	2,86%
Bachelors	11	3,54%	0	0,00%	0	0,00%	11	2,86%
Masters	95	30,55%	4	5,71%	0	0,00%	99	25,71%
Licentiate (master's Eq.)	173	55,63%	65	92,86%	0	0,00%	238	61,82%
Doctorate	15	4,82%	0	0,00%	2	50,00%	17	4,42%
Total	311		70		4		385	

Mean	5,47	5,97	5,75
Standard Dev.	1,01	0,34	3,20
Variance	1,02	0,12	10,25

What is your Professional Profile?

	Community		Authorities		Academia		Total	
Fishing Master LOA > 12 m	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Seafarer	2	0,64%	0	0,00%	0	0,00%	2	0,52%
Merchant Navy Officer	13	4,17%	0	0,00%	0	0,00%	13	3,36%
Shipping Officer	3	0,96%	0	0,00%	0	0,00%	3	0,78%
Navy Officer	0	0,00%	71	100,00%	0	0,00%	71	18,35%
Inspector	6	1,92%	0	0,00%	0	0,00%	6	1,55%
Shipping Manager	21	6,73%	0	0,00%	0	0,00%	21	5,43%
Administrator	35	11,22%	0	0,00%	0	0,00%	35	9,04%
Police	5	1,60%	0	0,00%	0	0,00%	5	1,29%
Auditor	9	2,88%	0	0,00%	0	0,00%	9	2,33%
Teacher	3	0,96%	0	0,00%	3	75,00%	6	1,55%
Academia Researcher	3	0,96%	0	0,00%	0	0,00%	3	0,78%
IT Technician	27	8,65%	0	0,00%	0	0,00%	27	6,98%
Cybersecurity Specialist	38	12,18%	0	0,00%	0	0,00%	38	9,82%
Network Administrator	12	3,85%	0	0,00%	0	0,00%	12	3,10%
Security Officer	44	14,10%	0	0,00%	0	0,00%	44	11,37%
Risk Management Specialist	19	6,09%	0	0,00%	0	0,00%	19	4,91%
Port Authority	7	2,24%	0	0,00%	0	0,00%	7	1,81%
Maritime Administrator	16	5,13%	0	0,00%	0	0,00%	16	4,13%
Insurance Agent	4	1,28%	0	0,00%	0	0,00%	4	1,03%
Insurance Inspector	6	1,92%	0	0,00%	0	0,00%	6	1,55%
Ship Owner	1	0,32%	0	0,00%	0	0,00%	1	0,26%
Naval Industry	16	5,13%	0	0,00%	0	0,00%	16	4,13%
Port Pilot	3	0,96%	0	0,00%	0	0,00%	3	0,78%
Ship Constructors	3	0,96%	0	0,00%	0	0,00%	3	0,78%
Ship Technology Providers	4	1,28%	0	0,00%	0	0,00%	4	1,03%
Lawyer	7	2,24%	0	0,00%	0	0,00%	7	1,81%
Total	312		71		4		387	

Mean	14,16	5,00	15,25
Standard Dev.	6,01	0,00	8,50
Variance	36,12	0,00	72,25

What is your Professional Field of Expertise?

	Community		Authorities		Academia		Total	
Cybersecurity	81	26,05%	0	0,00%	0	0,00%	81	20,98%
Physical Security	4	1,29%	0	0,00%	0	0,00%	4	1,04%
Information Security	28	9,00%	0	0,00%	0	0,00%	28	7,25%
Network Administration	16	5,14%	0	0,00%	0	0,00%	16	4,15%
Port Administration	33	10,61%	0	0,00%	0	0,00%	33	8,55%
Port Facility Operator	34	10,93%	0	0,00%	0	0,00%	34	8,81%
Ship Handling	10	3,22%	2	2,82%	0	0,00%	12	3,11%
Ship Operator	11	3,54%	0	0,00%	0	0,00%	11	2,85%
Academia	3	0,96%	1	1,41%	3	75,00%	7	1,81%
Ship Company Planning	19	6,11%	0	0,00%	0	0,00%	19	4,92%
Police and Investigation	6	1,93%	1	1,41%	0	0,00%	7	1,81%
Maritime Authority (AMN)	0	0,00%	66	92,96%	0	0,00%	66	17,10%
Insurances and salvages	18	5,79%	0	0,00%	0	0,00%	18	4,66%
Ship Construction	12	3,86%	0	0,00%	0	0,00%	12	3,11%
Ship Technology	26	8,36%	0	0,00%	0	0,00%	26	6,74%
Seafarer	1	0,32%	1	1,41%	0	0,00%	2	0,52%
Law and Rules Interpretation	6	1,93%	0	0,00%	0	0,00%	6	1,55%
Total	311		71		4		386	

Mean	6,47	11,86	11,25
Standard Dev.	5,05	1,03	4,50
Variance	25,55	1,07	20,25

For which entity do you work?

	Community		Authorities		Academia		Total	
AMN (Portuguese Maritime Authority)	0	0,00%	64	90,14%	0	0,00%	64	16,58%
Port Authority	27	8,68%	0	0,00%	0	0,00%	27	6,99%
Port Administration	24	7,72%	0	0,00%	0	0,00%	24	6,22%
Ship Company	32	10,29%	0	0,00%	0	0,00%	32	8,29%
Ship Handlers	36	11,58%	0	0,00%	0	0,00%	36	9,33%
Police Authority	10	3,22%	1	1,41%	0	0,00%	11	2,85%
Cybersecurity Company	18	5,79%	0	0,00%	0	0,00%	18	4,66%
Cybersecurity Authority	2	0,64%	0	0,00%	0	0,00%	2	0,52%
Academia	5	1,61%	1	1,41%	2	50,00%	8	2,07%
Certified Security Company	24	7,72%	0	0,00%	0	0,00%	24	6,22%
Port Facility Operator	70	22,51%	0	0,00%	0	0,00%	70	18,13%
Insurance Company	19	6,11%	0	0,00%	0	0,00%	19	4,92%
Ship Builders	12	3,86%	0	0,00%	0	0,00%	12	3,11%
Ship Maintenance and Repair	23	7,40%	0	0,00%	0	0,00%	23	5,96%
Salvage Company	4	1,29%	0	0,00%	0	0,00%	4	1,04%
Portuguese Navy	0	0,00%	5	7,04%	1	25,00%	6	1,55%
Total	311		71		4		386	

Mean	8,17	2,24	12,75
Standard Dev.	4,10	3,97	4,35
Variance	16,84	15,78	18,92

What do you consider about the existence of legislation concerning cybersecurity, specific for the Maritime Transport Sector in Portugal?

	Community		Authorities		Academia		Total	
Inexistent	31	9,90%	4	5,63%	1	25,00%	36	9,28%
Not enough	236	75,40%	38	53,52%	0	0,00%	274	70,62%
Enough	6	1,92%	0	0,00%	0	0,00%	6	1,55%
Complete	0	0,00%	1	1,41%	1	25,00%	2	0,52%
Very Complete	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Do not know	40	12,78%	28	39,44%	2	50,00%	70	18,04%
Total	313		71		4		388	

Mean	2,43	3,55	4,25
Standard Dev.	1,41	2,02	2,36
Variance	1,98	4,08	5,58

What do you consider about the existence of legislation concerning cybersecurity in Portugal?

	Community		Authorities		Academia		Total	
Inexistent	1	0,32%	0	0,00%	0	0,00%	1	0,26%
Not enough	57	18,15%	9	12,68%	1	25,00%	67	17,22%
Enough	190	60,51%	10	14,08%	0	0,00%	200	51,41%
Complete	2	0,64%	0	0,00%	1	25,00%	3	0,77%
Very Complete	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Do not know	63	20,06%	52	73,24%	2	50,00%	117	30,08%
Total	314		71		4		389	

Mean	3,43	5,07	4,50
Standard Dev.	1,37	1,57	1,91
Variance	1,88	2,47	3,67

What do you consider the existence of norms concerning cybersecurity, specific for the Maritime Transport Sector in Portugal?

	Community		Authorities		Academia		Total	
Inexistent	32	10,29%	3	4,23%	1	25,00%	36	9,33%
Not enough	230	73,95%	38	53,52%	0	0,00%	268	69,43%
Enough	8	2,57%	0	0,00%	0	0,00%	8	2,07%
Complete	0	0,00%	0	0,00%	1	25,00%	1	0,26%
Very Complete	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Do not know	41	13,18%	30	42,25%	2	50,00%	73	18,91%
Total	311		71		4		386	

Mean	2,45	3,65	4,25

Standard Dev.	1,43		2,04		2,36			
Variance	2,04		4,15		5,58			

What do you consider the existence of norms concerning cybersecurity in Portugal?

	Community		Authorities		Academia		Total	
Inexistent	1	0,32%	0	0,00%	0	0,00%	1	0,26%
Not enough	56	17,89%	9	12,68%	1	25,00%	66	17,01%
Enough	189	60,38%	10	14,08%	0	0,00%	199	51,29%
Complete	2	0,64%	0	0,00%	1	25,00%	3	0,77%
Very Complete	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Do not know	64	20,45%	52	73,24%	2	50,00%	118	30,41%
Total	313		71		4		388	

Mean	3,45		5,07		4,50			
Standard Dev.	1,38		1,57		1,91			
Variance	1,90		2,47		3,67			

What do you consider about the existence of standards concerning cybersecurity, specific for the Maritime Transport Sector in Portugal?

	Community		Authorities		Academia		Total	
Inexistent	33	10,58%	2	2,82%	1	25,00%	36	9,30%
Not enough	230	73,72%	39	54,93%	0	0,00%	269	69,51%
Enough	7	2,24%	0	0,00%	1	25,00%	8	2,07%
Complete	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Very Complete	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Do not know	42	13,46%	30	42,25%	2	50,00%	74	19,12%
Total	312		71		4		387	

Mean	2,46		3,66		4,00			
Standard Dev.	1,44		2,02		2,45			
Variance	2,08		4,08		6,00			

What do you consider about the existence of standards concerning cybersecurity in Portugal?

	Community		Authorities		Academia		Total	
Inexistent	1	0,32%	0	0,00%	0	0,00%	1	0,26%
Not enough	58	18,53%	10	14,08%	1	25,00%	69	17,78%
Enough	186	59,42%	8	11,27%	1	25,00%	195	50,26%
Complete	2	0,64%	0	0,00%	0	0,00%	2	0,52%
Very Complete	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Do not know	66	21,09%	53	74,65%	2	50,00%	121	31,19%
Total	313		71		4		388	

Mean	3,45		5,10		4,25			
Standard Dev.	1,38		1,58		2,06			
Variance	1,91		2,49		4,25			

To what extent do you agree with the existence of an agency in Portugal for the coordination of the response for the cyber events on the Maritime Transport Sector?

	Community		Authorities		Academia		Total	
Strongly disagree	2	0,64%	0	0,00%	0	0,00%	2	0,51%
Disagree	5	1,59%	1	1,41%	0	0,00%	6	1,54%
Neutral	4	1,27%	0	0,00%	0	0,00%	4	1,03%
Agree	291	92,68%	61	85,92%	3	75,00%	355	91,26%
Strongly agree	9	2,87%	7	9,86%	1	25,00%	17	4,37%
Do not know	3	0,96%	2	2,82%	0	0,00%	5	1,29%
Total	314		71		4		389	
Mean	3,98		4,13		4,25			
Standard Dev.	0,45		0,51		0,50			
Variance	0,20		0,26		0,25			

To what extent do you agree with the existence of an agency in Portugal to do a responsible disclosure and dissemination of the information concerning cyber events on the Maritime Transport Sector?

	Community		Authorities		Academia		Total	
Strongly disagree	1	0,32%	0	0,00%	0	0,00%	1	0,26%
Disagree	5	1,61%	1	1,41%	0	0,00%	6	1,55%
Neutral	1	0,32%	0	0,00%	1	20,00%	2	0,52%
Agree	294	94,84%	61	85,92%	3	60,00%	358	92,75%
Strongly agree	6	1,94%	8	11,27%	1	20,00%	15	3,89%
Do not know	3	0,97%	1	1,41%	0	0,00%	4	1,04%
Total	310		71		5		386	
Mean	3,99		4,11		4,00			
Standard Dev.	0,39		0,46		0,71			
Variance	0,16		0,22		0,50			

To what extent do you agree with the constitution of an Information Sharing and Analysis Centre (ISAC) in the Maritime Transport Sector?

	Community		Authorities		Academia		Total	
Strongly disagree	1	0,32%	0	0,00%	0	0,00%	1	0,26%
Disagree	1	0,32%	1	1,41%	0	0,00%	2	0,52%
Neutral	1	0,32%	0	0,00%	0	0,00%	1	0,26%
Agree	299	96,76%	62	87,32%	3	60,00%	364	94,55%
Strongly agree	6	1,94%	7	9,86%	1	20,00%	14	3,64%
Do not know	1	0,32%	1	1,41%	1	20,00%	3	0,78%
Total	309		71		5		385	
Mean	4,01		4,10		4,60			
Standard Dev.	0,28		0,45		0,89			
Variance	0,08		0,20		0,80			

To what extent do you agree that a public organism assumes the role of the ISAC for the Maritime Transport Sector coordinator?

	Community		Authorities		Academia		Total	
Strongly disagree	2	0,64%	0	0,00%	0	0,00%	2	0,52%
Disagree	8	2,56%	0	0,00%	0	0,00%	8	2,07%
Neutral	109	34,82%	0	0,00%	2	50,00%	111	28,68%
Agree	183	58,47%	63	90,00%	1	25,00%	247	63,82%
Strongly agree	7	2,24%	6	8,57%	1	25,00%	14	3,62%
Do not know	3	0,96%	1	1,43%	0	0,00%	4	1,03%
Total	313		70		4		387	
Mean	3,63		4,11		3,75			
Standard Dev.	0,68		0,36		0,96			
Variance	0,46		0,13		0,92			

To what extent do you agree that the ISAC Coordinator assumes the responsibility to conduct the responsible disclosure of the information concerning cyber events on the Maritime Transport Sector?

	Community		Authorities		Academia		Total	
Strongly disagree	1	0,32%	0	0,00%	0	0,00%	1	0,26%
Disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Neutral	1	0,32%	0	0,00%	1	25,00%	2	0,52%
Agree	298	95,82%	65	91,55%	2	50,00%	365	94,56%
Strongly agree	8	2,57%	5	7,04%	1	25,00%	14	3,63%
Do not know	3	0,96%	1	1,41%	0	0,00%	4	1,04%
Total	311		71		4		386	
Mean	4,03		4,10		4,00			
Standard Dev.	0,31		0,34		0,82			
Variance	0,10		0,12		0,67			

To what extent do you agree that the ISAC Coordinator assumes the coordination of the response for the cyber events on the Maritime Transport Sector?

	Community		Authorities		Academia		Total	
Strongly disagree	1	0,32%	0	0,00%	0	0,00%	1	0,26%
Disagree	1	0,32%	0	0,00%	0	0,00%	1	0,26%
Neutral	0	0,00%	0	0,00%	2	50,00%	2	0,52%
Agree	299	96,45%	65	91,55%	1	25,00%	365	94,81%
Strongly agree	5	1,61%	5	7,04%	1	25,00%	11	2,86%
Do not know	2	0,65%	1	1,41%	0	0,00%	3	0,78%
Total	310		71		4		385	
Mean	4,03		4,10		3,75			
Standard Dev.	0,38		0,34		0,96			
Variance	0,14		0,12		0,92			

To what extent do you agree that the AMN, in articulation with DGRM, assumes the role of ISAC Coordinator for the Maritime Transport Sector?

	Community		Authorities		Academia		Total	
Disagree	100	31,95%	1	1,39%	0	0,00%	101	25,96%
Agree	194	61,98%	65	90,28%	3	75,00%	262	67,35%
Do not know	17	5,43%	5	6,94%	1	25,00%	23	5,91%
Total	313		72		4		389	
Mean	1,75		2,08		2,25			
Standard Dev.	0,58		0,37		0,50			
Variance	0,34		0,13		0,25			

If you do not agree that AMN assumes the coordination role of the Maritime ISAC, in your opinion who should assume that role?

	Community		Authorities		Academia		Total	
Direção-Geral de Recursos Naturais, Segurança e Serviços Marítimos (DGRM)	51	50,50%	0	0,00%	0	0,00%	51	51,00%
Centro Nacional de Cibersegurança	48	47,52%	0	0,00%	0	0,00%	48	48,00%
Serviço de Estrangeiros e Fronteiras	1	0,99%	0	0,00%	0	0,00%	1	1,00%
Total	100		0		0		100	
Mean	1,65		0,00		0,00			
Standard Dev.	1,36		0,00		0,00			
Variance	1,85		0,00		0,00			

To what extent do you agree with the implementation of minimum cybersecurity requisites on the SSP, PFSP and PSP?

	Community		Authorities		Academia		Total	
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	1	0,32%	0	0,00%	0	0,00%	1	0,26%
Neutral	1	0,32%	0	0,00%	0	0,00%	1	0,26%
Agree	294	94,84%	60	84,51%	2	50,00%	356	92,47%
Strongly agree	11	3,55%	11	15,49%	1	25,00%	23	5,97%
Do not know	3	0,97%	0	0,00%	1	25,00%	4	1,04%
Total	310		71		4		385	
Mean	4,05		4,15		4,75			
Standard Dev.	0,30		0,36		0,96			
Variance	0,09		0,13		0,92			

To what extent do you agree with the implementation of the prerequisite to executing a CSA and a CSP becoming annexes of the SSP, PFSP and PSP?

	Community		Authorities		Academia		Total	
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	1	0,32%	1	1,43%	0	0,00%	2	0,52%
Neutral	1	0,32%	0	0,00%	0	0,00%	1	0,26%
Agree	289	93,83%	61	87,14%	1	25,00%	351	91,88%
Strongly agree	12	3,90%	8	11,43%	1	25,00%	21	5,50%
Do not know	4	1,30%	0	0,00%	2	50,00%	6	1,57%
Total	308		70		4		382	
Mean	4,06		4,09		5,25			
Standard Dev.	0,36		0,41		0,96			
Variance	0,13		0,17		0,92			

To what extent do you agree with the following definition:
Ships Cybersecurity officer (SCySO) - The person or persons tasked to manage and coordinate the cybersecurity of a ship. For larger fleets, the SCySO is likely to report to the Company's Chief Information Security Officer (CISO) or CSO, for smaller fleets the role is likely to report to the Company's Head of Security.

	Community		Authorities		Academia		Total	
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Neutral	2	0,65%	2	2,86%	1	25,00%	5	1,31%
Agree	290	93,85%	62	88,57%	0	0,00%	352	91,91%
Strongly agree	6	1,94%	5	7,14%	2	50,00%	13	3,39%
Do not know	11	3,56%	1	1,43%	1	25,00%	13	3,39%
Total	309		70		4		383	
Mean	4,08		4,07		4,75			
Standard Dev.	0,40		0,39		1,26			
Variance	0,16		0,15		1,58			

To what extent do you agree with the following definition:
Cybersecurity Assessment (CSA) - Assessing the cybersecurity of ship assets requires specialist knowledge and expertise and as such, it is recommended that suitably qualified and experienced individuals undertake the preparation of the CSA and CSP.

	Community		Authorities		Academia		Total	
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	1	0,32%	0	0,00%	0	0,00%	1	0,26%
Neutral	2	0,65%	0	0,00%	0	0,00%	2	0,52%
Agree	284	92,21%	63	90,00%	1	25,00%	348	91,10%
Strongly agree	9	2,92%	7	10,00%	2	50,00%	18	4,71%
Do not know	12	3,90%	0	0,00%	1	25,00%	13	3,40%
Total	308		70		4		382	
Mean	4,09		4,10		5,00			

Standard Dev.	0,44	0,30	0,82
Variance	0,20	0,09	0,67

To what extent do you agree with the following definition:
Cybersecurity Plan (CSP) - The ship security assessments form the basis of the security plans for the ship. These plans should address the pre-dominantly physical and personnel issues identified in the relevant assessment through the establishment of appropriate security measures designed to minimise the likelihood of a breach of security and the consequences of potential risks. It is intended that wherever appropriate the CSP will build upon the existing ship security plan (SSP) and become an annexe to it.

	Community		Authorities		Academia		Total	
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Neutral	2	0,65%	0	0,00%	0	0,00%	2	0,52%
Agree	287	93,18%	65	92,86%	1	33,33%	353	92,65%
Strongly agree	8	2,60%	5	7,14%	1	33,33%	14	3,67%
Do not know	11	3,57%	0	0,00%	1	33,33%	12	3,15%
Total	308		70		3		381	

Mean	4,09	4,07	5,00
Standard Dev.	0,41	0,26	1,00
Variance	0,17	0,07	1,00

To what extent do you agree with the following definition:
Cybersecurity officer (CS officer) - The person or persons tasked to manage and coordinate the cybersecurity in a port/port facility. For larger ports, the CS officer is likely to report to the chief information security officer (CISO). For smaller ports, the role is likely to report to the Head of Security.

	Community		Authorities		Academia		Total	
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	2	0,65%	0	0,00%	0	0,00%	2	0,53%
Neutral	3	0,98%	0	0,00%	0	0,00%	3	0,79%
Agree	284	92,51%	63	90,00%	1	33,33%	348	91,58%
Strongly agree	7	2,28%	6	8,57%	1	33,33%	14	3,68%
Do not know	10	3,26%	1	1,43%	1	33,33%	12	3,16%
Total	307		70		3		380	

Mean	4,07	4,11	5,00
Standard Dev.	0,46	0,36	1,00
Variance	0,21	0,13	1,00

To what extent do you agree with the following definition:
Port Facility / Port Cybersecurity Assessment (CSA): The port and port facility should first assess each of the vulnerability and countermeasures identified in the respective final port/port facility assessment reports to establish whether there are cybersecurity implications arising from them. It is intended that wherever appropriate the CSA should build upon the existing security assessments.

	Community		Authorities		Academia		Total	
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Neutral	2	0,65%	2	2,86%	0	0,00%	4	1,05%
Agree	290	94,16%	66	94,29%	1	25,00%	357	93,46%
Strongly agree	6	1,95%	2	2,86%	2	50,00%	10	2,62%
Do not know	10	3,25%	0	0,00%	1	25,00%	11	2,88%
Total	308		70		4		382	
Mean	4,08		4,00		5,00			
Standard Dev.	0,39		0,24		0,82			
Variance	0,15		0,06		0,67			

To what extent do you agree with the following definition:
Port Facility / Port cybersecurity plan (CSP): The security assessments form the basis of the security plans for the port and port facilities. These plans should address the issues identified in the relevant assessment through the establishment of appropriate security measures designed to minimize the likelihood of a breach of security and the consequences of potential risks. It is intended that wherever appropriate the CSP will build upon the existing port facility/port security plan (PFSP/PSP).

	Community		Authorities		Academia		Total	
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Neutral	2	0,65%	1	1,43%	0	0,00%	3	0,79%
Agree	290	94,16%	65	92,86%	1	25,00%	356	93,19%
Strongly agree	7	2,27%	4	5,71%	2	50,00%	13	3,40%
Do not know	9	2,92%	0	0,00%	1	25,00%	10	2,62%
Total	308		70		4		382	
Mean	4,07		4,04		5,00			
Standard Dev.	0,38		0,27		0,82			
Variance	0,14		0,07		0,67			

Do you know the publication: "IET Standards - Code of Practice: Cyber Security for Ships", of 2017?

	Community		Authorities		Academia		Total	
Yes	190	60,90%	17	24,29%	0	0,00%	207	53,63%
No	122	39,10%	53	75,71%	4	100,00%	179	46,37%
Total	312		70		4		386	
Mean	1,39		1,76		2,00			
Standard Dev.	0,49		0,43		0,00			
Variance	0,24		0,19		0,00			

To what extent do you agree with their adaptation and implementation of the "IET Standards - Code of Practice: Cyber Security for Ships", of 2017, in Portugal?

	Community		Authorities		Academia		Total	
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	9	4,71%	0	0,00%	0	0,00%	9	4,31%
Neutral	74	38,74%	2	11,11%	0	0,00%	76	36,36%
Agree	105	54,97%	16	88,89%	0	0,00%	121	57,89%
Strongly agree	2	1,05%	0	0,00%	0	0,00%	2	0,96%
Do not know	1	0,52%	0	0,00%	0	0,00%	1	0,48%
Total	191		18		0		209	
Mean	3,54		3,89		0,00			
Standard Dev.	0,63		0,32		0,00			
Variance	0,40		0,10		0,00			

Do you know the publication: "IET Standards – Code of Practice: Cyber Security for Ports and Port Systems", of 2016

	Community		Authorities		Academia		Total	
Yes	193	62,06%	18	25,35%	0	0,00%	211	54,66%
No	118	37,94%	53	74,65%	4	100,00%	175	45,34%
Total	311		71		4		386	
Mean	1,38		1,75		2,00			
Standard Dev.	0,49		0,44		0,00			
Variance	0,24		0,19		0,00			

To what extent do you agree with their adaptation and implementation of the "IET Standards – Code of Practice: Cyber Security for Ports and Port Systems", of 2016, in Portugal?

	Community		Authorities		Academia		Total	
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	8	4,17%	0	0,00%	0	0,00%	8	3,83%
Neutral	67	34,90%	2	11,76%	0	0,00%	69	33,01%
Agree	115	59,90%	15	88,24%	0	0,00%	130	62,20%
Strongly agree	2	1,04%	0	0,00%	0	0,00%	2	0,96%
Do not know	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Total	192		17		0		209	
Mean	3,58		3,88		0,00			
Standard Dev.	0,59		0,33		0,00			
Variance	0,35		0,11		0,00			

Do you agree with the implementation of cybersecurity helpdesks on the main harbours?

	Community		Authorities		Academia		Total	
Yes	257	99,61%	44	100,00%	0	0,00%	301	99,67%
No	1	0,39%	0	0,00%	0	0,00%	1	0,33%
Total	258		44		0		302	
Mean	1,00		1,00		0,00			
Standard Dev.	0,06		0,00		0,00			
Variance	0,00		0,00		0,00			

Do you agree that the helpdesks help to prepare for the cybersecurity inspections to a specific:

	Community		Authorities		Academia		Total	
Ship								
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	1	0,33%	0	0,00%	0	0,00%	1	0,27%
Neutral	3	0,99%	1	1,47%	0	0,00%	4	1,07%
Agree	294	96,71%	63	92,65%	2	66,67%	359	95,73%
Strongly agree	6	1,97%	4	5,88%	1	33,33%	11	2,93%
Total	304		68		3		375	
Mean	4,00		4,04		4,33			
Standard Dev.	0,21		0,27		0,58			
Variance	0,04		0,07		0,33			
	Community		Authorities		Academia		Total	
Port Facility								
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Neutral	1	0,33%	1	1,47%	0	0,00%	2	0,53%
Agree	297	97,70%	62	91,18%	2	66,67%	361	96,27%
Strongly agree	6	1,97%	5	7,35%	1	33,33%	12	3,20%

Total	304		68		3		375	
Mean	4,02		4,06		4,33			
Standard Dev.	0,15		0,29		0,58			
Variance	0,02		0,09		0,33			
	Community		Authorities		Academia		Total	
Port								
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Neutral	1	0,33%	1	1,47%	0	0,00%	2	0,53%
Agree	297	97,70%	63	92,65%	2	66,67%	362	96,53%
Strongly agree	6	1,97%	4	5,88%	1	33,33%	11	2,93%
Total	304		68		3		375	
Mean	4,02		4,04		4,33			
Standard Dev.	0,15		0,27		0,58			
Variance	0,02		0,07		0,33			

Do you agree that the helpdesks provide support to the elaboration and implementation of training plans to a specific:

	Community		Authorities		Academia		Total	
Ship								
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	2	0,66%	0	0,00%	0	0,00%	2	0,53%
Neutral	3	0,99%	1	1,47%	0	0,00%	4	1,06%
Agree	291	95,72%	63	92,65%	3	75,00%	357	94,95%
Strongly agree	8	2,63%	4	5,88%	1	25,00%	13	3,46%
Total	304		68		4		376	
Mean	4,00		4,04		4,25			
Standard Dev.	0,25		0,27		0,50			
Variance	0,06		0,07		0,25			
	Community		Authorities		Academia		Total	
Port Facility								
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	1	0,33%	0	0,00%	0	0,00%	1	0,27%
Neutral	1	0,33%	1	1,47%	1	25,00%	3	0,80%
Agree	294	97,03%	61	89,71%	2	50,00%	357	95,20%
Strongly agree	7	2,31%	6	8,82%	1	25,00%	14	3,73%
Total	303		68		4		375	
Mean	4,01		4,07		4,00			
Standard Dev.	0,20		0,31		0,82			
Variance	0,04		0,10		0,67			
	Community		Authorities		Academia		Total	
Port								

Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	1	0,33%	0	0,00%	0	0,00%	1	0,27%
Neutral	1	0,33%	1	1,47%	1	25,00%	3	0,80%
Agree	294	97,03%	62	91,18%	2	50,00%	358	95,47%
Strongly agree	7	2,31%	5	7,35%	1	25,00%	13	3,47%
Total	303		68		4		375	

Mean	4,01	4,06	4,00
Standard Dev.	0,20	0,29	0,82
Variance	0,04	0,09	0,67

Do you agree that the helpdesks, if requested by the operator, to conduct cybersecurity exercises to a specific :

	Community		Authorities		Academia		Total	
Ship								
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Neutral	4	1,32%	1	1,47%	1	25,00%	6	1,60%
Agree	293	96,38%	62	91,18%	1	25,00%	356	94,68%
Strongly agree	7	2,30%	5	7,35%	2	50,00%	14	3,72%
Total	304		68		4		376	

Mean	4,01	4,06	4,25
Standard Dev.	0,19	0,29	0,96
Variance	0,04	0,09	0,92

	Community		Authorities		Academia		Total	
Port Facility								
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Neutral	1	0,33%	1	1,47%	1	25,00%	3	0,80%
Agree	294	97,35%	61	89,71%	1	25,00%	356	95,19%
Strongly agree	7	2,32%	6	8,82%	2	50,00%	15	4,01%
Total	302		68		4		374	

Mean	4,02	4,07	4,25
Standard Dev.	0,16	0,31	0,96
Variance	0,03	0,10	0,92

	Community		Authorities		Academia		Total	
Port								
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Neutral	1	0,33%	1	1,47%	1	25,00%	3	0,80%
Agree	292	97,01%	62	91,18%	1	25,00%	355	95,17%
Strongly agree	8	2,66%	5	7,35%	2	50,00%	15	4,02%
Total	301		68		4		373	

Mean	4,02	4,06	4,25
Standard Dev.	0,17	0,29	0,96
Variance	0,03	0,09	0,92

Do you agree that the helpdesks to provide cybersecurity validations to a specific :

	Community		Authorities		Academia		Total	
Ship								
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	2	0,66%	0	0,00%	0	0,00%	2	0,53%
Neutral	2	0,66%	1	1,47%	1	33,33%	4	1,07%
Agree	293	96,38%	63	92,65%	1	33,33%	357	95,20%
Strongly agree	7	2,30%	4	5,88%	1	33,33%	12	3,20%
Total	304		68		3		375	

Mean	4,00	4,04	4,00
Standard Dev.	0,24	0,27	1,00
Variance	0,06	0,07	1,00

	Community		Authorities		Academia		Total	
Port Facility								
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	2	0,66%	0	0,00%	0	0,00%	2	0,53%
Neutral	2	0,66%	1	1,47%	1	33,33%	4	1,07%
Agree	292	96,37%	64	94,12%	1	33,33%	357	95,45%
Strongly agree	7	2,31%	3	4,41%	1	33,33%	11	2,94%
Total	303		68		3		374	

Mean	4,00	4,03	4,00
Standard Dev.	0,24	0,24	1,00
Variance	0,06	0,06	1,00

	Community		Authorities		Academia		Total	
Port								
Strongly disagree	0	0,00%	0	0,00%	0	0,00%	0	0,00%
Disagree	2	0,66%	0	0,00%	0	0,00%	2	0,53%
Neutral	1	0,33%	2	2,94%	1	33,33%	4	1,07%
Agree	293	96,70%	63	92,65%	1	33,33%	357	95,45%
Strongly agree	7	2,31%	3	4,41%	1	33,33%	11	2,94%
Total	303		68		3		374	

Mean	4,01	4,01	4,00
Standard Dev.	0,23	0,27	1,00
Variance	0,05	0,07	1,00

To what extent do you agree that should be held a national cybersecurity exercise on the Maritime Domain at least once a year?

	Community		Authorities		Academia		Total	
Yes	299	95,53%	66	84,62%	2	40,00%	367	98,13%
No	5	1,60%	1	1,28%	1	20,00%	7	1,87%
Total	304		67		3		374	
Mean	1,07		1,29		2,00			
Standard Dev.	0,35		0,70		1,00			
Variance	0,13		0,50		1,00			

Do you agree that the helpdesks have cybersecurity specialized teams to conduct the inspections to the:

	Community		Authorities		Academia		Total	
Ships								
Strongly disagree	1	0,33%	0	0,00%	0	0,00%	1	0,27%
Disagree	6	1,97%	0	0,00%	0	0,00%	6	1,59%
Neutral	3	0,98%	1	1,47%	1	25,00%	5	1,33%
Agree	287	94,10%	65	95,59%	2	50,00%	354	93,90%
Strongly agree	8	2,62%	2	2,94%	1	25,00%	11	2,92%
Total	305		68		4		377	
Mean	3,97		4,01		4,00			
Standard Dev.	0,38		0,21		0,82			
Variance	0,14		0,04		0,67			
	Community		Authorities		Academia		Total	
Port Facilities								
Strongly disagree	1	0,33%	0	0,00%	0	0,00%	1	0,27%
Disagree	5	1,65%	0	0,00%	0	0,00%	5	1,33%
Neutral	3	0,99%	1	1,47%	1	25,00%	5	1,33%
Agree	287	94,72%	64	94,12%	2	50,00%	353	94,13%
Strongly agree	7	2,31%	3	4,41%	1	25,00%	11	2,93%
Total	303		68		4		375	
Mean	3,97		4,03		4,00			
Standard Dev.	0,36		0,24		0,82			
Variance	0,13		0,06		0,67			
	Community		Authorities		Academia		Total	
Ports								
Strongly disagree	1	0,33%	0	0,00%	0	0,00%	1	0,27%
Disagree	5	1,64%	0	0,00%	0	0,00%	5	1,33%
Neutral	3	0,98%	2	2,99%	1	25,00%	6	1,60%
Agree	289	94,75%	63	94,03%	2	50,00%	354	94,15%
Strongly agree	7	2,30%	2	2,99%	1	25,00%	10	2,66%
Total	305		67		4		376	

Mean	3,97	4,00	4,00
Standard Dev.	0,36	0,25	0,82
Variance	0,13	0,06	0,67

To what extent do you agree on the existence of recognized, by DGRM and CNCS, security organisations to conduct the port and ships inspections?

	Community		Authorities		Academia		Total	
Strongly disagree	4	1,30%	1	1,39%	0	0,00%	5	1,31%
Disagree	3	0,98%	24	33,33%	1	25,00%	28	7,31%
Neutral	8	2,61%	4	5,56%	1	25,00%	13	3,39%
Agree	285	92,83%	39	54,17%	1	25,00%	325	84,86%
Strongly agree	5	1,63%	3	4,17%	1	25,00%	9	2,35%
Do not know	2	0,65%	0	0,00%	0	0,00%	2	0,52%
Total	307		72		4		383	

Mean	3,94	3,32	3,50
Standard Dev.	0,47	1,11	1,29
Variance	0,22	1,23	1,67

To what extent do you agree on the existence of recognized, by DGRM and CNCS, security organisations to conduct the port and ships security plans?

	Community		Authorities		Academia		Total	
Strongly disagree	3	0,98%	1	1,45%	0	0,00%	4	1,06%
Disagree	3	0,98%	24	34,78%	0	0,00%	27	7,12%
Neutral	8	2,61%	4	5,80%	0	0,00%	12	3,17%
Agree	284	92,81%	38	55,07%	2	50,00%	324	85,49%
Strongly agree	4	1,31%	2	2,90%	1	25,00%	7	1,85%
Do not know	3	0,98%	0	0,00%	1	25,00%	4	1,06%
Total	306		69		4		379	

Mean	3,97	3,23	4,75
Standard Dev.	0,48	1,02	0,96
Variance	0,23	1,03	0,92

To what extent do you agree that the approval of the CSA and CSP should be done by the DGRM after CNCS and AMN issued their opinion (in case of the Port Facilities and Ports the CCPP also must issue is an opinion on the cybersecurity assessment and plan), in accordance with the Decree-Law 226/06, of 15 November?

	Community		Authorities		Academia		Total	
Strongly disagree	2	0,66%	0	0,00%	0	0,00%	2	0,53%
Disagree	2	0,66%	1	1,49%	1	25,00%	4	1,06%
Neutral	5	1,64%	2	2,99%	1	25,00%	8	2,13%
Agree	285	93,44%	60	89,55%	1	25,00%	346	92,02%
Strongly agree	4	1,31%	3	4,48%	0	0,00%	7	1,86%
Do not know	7	2,30%	1	1,49%	1	25,00%	9	2,39%
Total	305		67		4		376	

Mean	4,01	4,01	3,75
Standard Dev.	0,46	0,44	1,71
Variance	0,21	0,20	2,92