Assuring Cybersecurity on the Maritime Domain

Implementation of a Functional Organization to Address the Cybersecurity on the Maritime Domain

Extensive Summary of the Thesis

Sérgio Ricardo Caldeira de Carvalho

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 on-shore 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 with the directives on the water transports and maritime domain in general.

The Research Question and Hypotheses

To define the basis for this organisation, it was purposed to answer 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 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 organisation 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.

The analysis model

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 interconnect model of these three theories will help us to understand the organisations adopted by the countries to tackle the cybersecurity issue and to adopt, adapt or design a model to implement on Portugal.

Table 1 - 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

In table 1, we can see the interconnection between these theories. To integrate the mentioned theories in a single view, we could schematize as following:

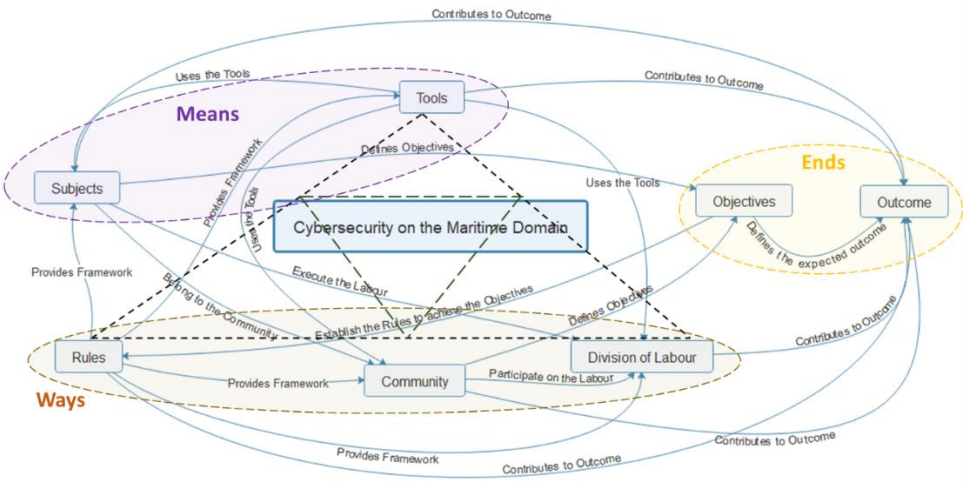

Figure 1 - An integrated schema of Grand Strategy, AT and ANT

The Countries Chosen for the Background Search

In the background search, we will analyse the organisation created to deal with the cybersecurity on the Maritime Domain. To select those countries was verified by several factors and assumed some premises that conditioned the selection.

- 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.

The first source used for the triage was the Global Cybersecurity Index (GCI), 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

To narrow down the number of countries, we used the UN e-Government Development Index (EGDI), that is also an important index to sort the nations regarding the digital footprint; it is a benchmarking tool that provides a comparative assessment of the e-government development of UN Member States.

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.

This supposition is based on several studies that state that organisational culture influences the organisational structure. This influence, mainly in multicultural organisations, can lead to new initiatives and good production rates but needs a disruptive implementation, but this always brings resistance to change, and difficulties to implement a non-indigenous culture-based organisational structure.

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, decision making, and by the normal organisational structures adopted.

Considering what was previously stated and that after initial research, it was clear that the legal framework constraints 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 conditioned the organisational structure choices made by the countries. For these facts, we can state that the legal framework has a fulcra role in the organisational structure and outcome.

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.

The Analysis Results of the Background Research

In the USA, we could see that the USA approach to assure the cybersecurity on the Maritime Transport System (MTS) is through the existing organisation of the United States Coast Guard (USCG), been the 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.

The French, Spanish and UK approach to assure the cybersecurity on the maritime domains was through the already existing organisation for the implementation and verification of the security on the maritime domain, updating the existing legal framework and adopting the EU and IMO regulations to add the cyber factor to security. These countries have a more complex organisation than the United States concerning the implementation and verification of the cybersecurity on the maritime domain, which in the USA is centralised on the USCG but in the EU countries are divided by several agencies. However, all the countries studied used the already implemented organisation to verify the security of the vessels and the facilities.

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.

The Portuguese Reality

In conclusion, Portuguese reality has specific regulations concerning cybersecurity in general but lacks a doctrine concerning the maritime sector.

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 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 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 organization. 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 Proposed Model

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 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 (annexe of the SSA, PFSA, PSA) and CSP (annexe 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 cyber-security 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.

The Proposed Model Validation

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

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.

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.

The Questionnaire Structure

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

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.

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.

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.

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 references UK publications of cybersecurity in the maritime domain.

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.

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.

Validating the Questionnaire

In the questionnaire 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.

Analysis of the Questionnaires Results

The participation of the questionnaire, not considering the Academia Group, allowed a sampling error of 5%. The minimum participation in obtaining the 5% sample error is:

Table 2 - 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

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

The Maritime Community:

- Has 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, leading to the adoption of the proposed model in this thesis, and so we can conclude that the Maritime Community approves the proposed model.

Conclusions

To be able to answer 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 first hypothesis was proved through the analysis of 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 the fact that EU Directives are mandatorily transposed to national law.

The second hypothesis was answered throughout “State of the Art” analysis. 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 the 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.

The third hypothesis was also answered in “State of the Art” and in the Portuguese reality analysis. 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 of the “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.

The fourth hypothesis was validated in the analysis and considerations done to build the proposed model and in the validation of the model itself. In the proposed model development 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.

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 functional organisation to address the cybersecurity on the Portuguese Maritime Domain was answered with the proposed model, establishing a model of the targeted functional organisation, and we successfully validated that model through the questionnaire results. 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 on the Portuguese Maritime Domain.