CHALMERS
UNIVERSITY OF TECHNOLOGY

Building Barriers, but for whom

Compliance of Swedish port organisations towards security regulations: a case study

Master's thesis in the Master's Programme Maritime Management

SEBASTIAN COLE
PHILIP WINBERG

Department of Mechanics and Maritime Sciences
Division of Maritime Studies
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2018
Report No. 2018-74

REPORT NO. 2018:74

Building Barriers, but for whom
Compliance of Swedish port organisations towards security regulations: a case study

SEBASTIAN COLE & PHILIP WINBERG

Department of Mechanics and Maritime Sciences
Division of Maritime Studies
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2018

Building Barriers, but for whom
Compliance of Swedish port organisations towards security regulations: a case study

SEBASTIAN COLE
PHILIP WINBERG

Report No. 2018-74

Department of Mechanics and Maritime Sciences
Division of Maritime Studies
Chalmers University of Technology
SE-412 96 Gothenburg
Sweden
Telephone: +46 (0)31–772 1000

Chalmers Reproservice
Gothenburg, Sweden 2018

ABSTRACT

The impacts of the terrorist attacks on 11th of September 2001 in New York had a profound effect and the aftermath embraced universal consequences and repercussions. It was perceived by the International Maritime Organization and the European Union that similar attacks could be imminent and both bodies rapidly adopted new maritime and port security regulations to avert further events occurring. On a local level, the Member States of the two bodies had to develop their own national regulations. In this context, the thesis focuses on the barriers that Swedish port organisations have identified in order to comply with the regulatory security framework on a global, international and national level. Using a deductive approach, this explanatory case study is based on a wide electronic survey targeted at public port organisations in Sweden. The survey was based on the theoretical framework constructed. Furthermore, in-depth interviews were conducted with a wide range of special advisers and experts in the field of study. From this research, two main findings emerged; while the current regulatory security framework is sound, this still requires that all parties are actively involved. For all parties to be actively involved, the knowledge-creation and information-sharing must be improved on both an inter- and intra-organisational level.

KEYWORDS: Barriers; information-sharing; knowledge-creation; lack of resources; maritime and port security; port organisations; regulatory compliance; regulatory security framework; security culture; security network

ACKNOWLEDGEMENTS

This master research was conducted from early January 2018 to early June 2018 as part of the Masters' Degree programme delivered and supervised under the Department of Mechanics and Maritime Sciences at Chalmers University of Technology in Gothenburg, Sweden. The thesis was written as the final research project under the Master Degree's Maritime Management programme.

Firstly, we wish to thank our supervisor Dr Henrik Ringsberg at the Department of Engineering at the University of Borås. Henrik, your profound knowledge and experience of academic research, your sincere enthusiasm and wise guidance, and your welcome encouragement along the way have all been truly appreciated.

Furthermore, we would like to thank all those in the ports who have taken time from their busy schedules to answer our research survey while additionally thanking all those interviewed respondents who have given us their valuable time and trust in sharing their knowledge, views and opinions on the subject.

Moreover, we would like to thank the experts in various fields who collectively have overseen our research. It has been a true honour to have had these prominent persons show such willingness to enhance the academic value of our study with their comments and observations.

Finally, we would like to thank our families and friends for the support they have given us during this demanding and intensive period. A very special "thanks" also goes to our respective patient and precious partners, Johanna and Charlotte.

Stockholm and Gothenburg, 2018

Sebastian Cole and Philip Winberg

LIST OF ABBREVIATIONS

EC	European Commission
ECCRI	European Code of Conduct for Research Integrity
EEZ	Exclusive Economic Zone
EU	European Union
HRO	High Reliability Organisation
IMO	International Maritime Organization
ISPS Code	International Ship and Port Facility Security Code
Lo-Lo	Lift-on Lift-off
MSC	Maritime Safety Committee
Pax	Passengers
PFSA	Port Facility Security Assessment
PFSO	Port Facility Security Officer
PFSP	Port Facility Security Plan
PoS	Ports of Sweden
Ro-Ro	Roll-on Roll-off
SCA	Swedish Customs Agency
SCG	Swedish Coast Guard
SMA	Swedish Maritime Authority
SOLAS	International Convention for the Safety of Life at Sea
SPA	Swedish Police Authority
STA	Swedish Transport Agency
UN	United Nations
UNCLOS	United Nations Convention of the Law of the Sea
US	United States
USCG	United States Coast Guard

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

In the following chapter the reader is provided with an introduction to the thesis. Firstly, the background is presented and the reasons for conducting the research are given, which include the identification of gaps in the academia that this study intends to reveal. Secondly, the purpose of the report is presented, followed by the research questions necessary to achieve the objectives of the study. Finally, the limitations are considered and presented.

1.1 Background

The impact of the terrorist attacks on 11th September 2001 in New York had a profound effect and the aftermath embraced truly universal consequences and repercussions. Subsequently, humanity had never previously experienced such drastic outcomes caused by only a few extreme fundamentalists and society has not been the same since. The events paralyzed an entire world, forcing it to ask how this was allowed to happen. As a result, that question would drive the world into re-shaping and engaging in the way security and risk assessment is now viewed and executed (International Maritime Organization, n.d.). Simultaneously, a continuous globalisation has been taking place. The maritime industry, which represents 90 percent of all globally traded goods, is a major pillar for this and necessary for international trade to continue and thrive (International Chamber of Shipping, 2017). Therefore, the shipping sector stood, and is now standing before, a major challenge; to allow and augment business across continents, nations and cultures, while concurrently meeting the new and high demands of security that are in place in the wake of today's terrorism.

The outcome of the events above, is evident when viewing how ports functioned before and after 9/11. Historically, ports were designed to allow for easy access to provide business and trade to take place. Today, however, at least in theory, ports are closed entities (Christopher, 2014). This sudden change in port security is also evident when reviewing how current port security regulations have been implemented, and the rapidity in which this has been done. For example, the International Ship and Port Facility Security Code (ISPS Code) entered into force in 2004, just eighteen months after its adoption, and is to date, the swiftest ever maritime related code to do so (International Maritime Organization, n.d.). Further, the European Commission (EC) agreed with its contents and enhanced Regulation 725/2004 and Directive 2005/65/EC, concerning the security of ships and ports in the same space of time (EUR-Lex, 2016). As a result, many Sovereign States, Sweden for instance, have followed suit and implemented a regulatory framework of their own shortly after (Swedish Maritime Administration, n.d.).

In the urgency of implementing security standards on the global, international, national levels, no wider coherence or strategy to align the various initiatives has taken place (in all but a few cases). Neither, have the stakeholders been consulted or asked to contribute in making the regulations feasible and compelling (Papa, 2012). This has made the regulatory security framework fragmented across the supply chain and has left many stakeholders side-lined, but still required to conform, if they wish to successfully continue trading.

Hence, as the maritime transportation industry and its ports are key components in the international flow of goods, enabling today's globalised world to trade and exist (Helmick, 2008), it has a strategic value and importance in the socio-economical relationship among States (Notteboom, 2011). According to Urciuoli et al. (2013), and Bichou (2004) this multiple-stakeholder environment, where international businesses and organisations unceasingly interact, security related issues are generally regarded as greatly significant when ensuring continuous efficiency of port operations. Furthermore, port infrastructures and cargo handling operations are not only subject to terrorism, as discussed above, but other criminal activities, such as the smuggling of illegal commodities, trafficking and pilfering. In short, it is of vital importance for port organisations across the globe to maintain a certain level of security in order to eradicate or limit the risks of such events to materialise and allow supply chains to continue their progress (Bichou, 2004, Urciuoli et al., 2013).

To consolidate in this field, published research that addresses port security and compliance with regulatory frameworks shows that one of the major problems for the successful implementation of such legislations are the limitations or restraints due to the cost-related issues. In return, this can relate to the miscorrelation between supply-chain efficiency and security (Mazaheri and Ekwall, 2009, Burns, 2013, Mileski et al., 2015). Furthermore, academia also discusses the lack of general and comprehensive methodologies for risk assessments and the implementation of security regulations within the maritime industry (Yanga et al., 2013, Romero-Faza and Camarero-Orive, 2017).

However, published research which emphasizes on barriers that potentially exist in complying with the regulatory security framework is lacking. Moreover, from a Swedish perspective, studies have been conducted regarding the implementation of the ISPS Code (Mazaheri and Ekwall, 2009, Hellberg, 2009), but have focused on the economic resources required for implementation. Here, a shortage of publications on the full compliance of all security regulations, together with potential barriers, has been identified. This thesis will therefore present a framework of security regulations. In addition, it will also aim to identify the potential barriers that exist in order to comply with the regulatory framework and focus more in depth on how knowledge-creation and information-sharing may be contributing factors in complying from a Swedish port perspective.

In this respect, a relevant research project, HAZARD, is currently underway and aims to mitigate the effects of emergencies in major seaports in the Baltic Sea Region. In particular, the objective of the project's Work Package 3 is the "better compliance and implementation of existing and future regulations". It is hoped that this thesis might be able to contribute towards the HAZARD project.

1.2 Purpose

The purpose of this research is two-fold; [1] to present a theoretical framework for the evaluation of the regulatory framework for maritime and port security at the global, international and national levels, and [2] to identify barriers in the legal compliance of the regulatory security framework for Swedish port organisations.

1.3 Research Questions

To achieve the above stated purpose, three areas of importance have been recognised. The first area is to identify which regulations control the decision-making for port organisations in Sweden. Furthermore, the second area of importance to the purpose is to identify potential barriers in order for Swedish ports to achieve compliance with all the relevant regulations. Thirdly, further research will be conducted regarding two potential barriers, namely knowledge-creation and information-sharing.

The identified areas of importance were divided into the following two research questions:

- What are the main barriers that limit Swedish port organisations' abilities to successfully comply with the regulatory framework for maritime and port security at the global, international and national levels?

- How does knowledge-creation and information-sharing correlate with Swedish port organisations' abilities to successfully comply with the regulatory framework for maritime and port security at the global, international and national levels?

1.4 Limitations

Many security regulations for ports exist across the globe. In pursuance of the project purpose, the thesis was limited to reviewing the regulatory security framework in each of the following categories; global, international and national. All the reviewed regulations were required to have a mandate in Sweden.

Moreover, as the research purpose states, only Swedish public ports were asked to partake in the study. The reasoning behind the geographical limitation is the time constraint. It was also regarded that the restriction of only viewing one single State's ports, would allow for a qualitative and reliable analysis to be conducted and will eliminate potential research noise, such as nationwide culture, domestic resources and the State's view on the importance of implementation and the compliance of the regulations.

Since, the thesis project focussed on mandatory regulations and legislations for port security in Sweden, the port organisations asked to participate in the study were be public ports in the category obligated to comply with the ISPS Code according to the code's own definition.

2 RESEARCH METHODOLOGY

In the following chapter, the research methodology is presented to the reader. An introduction to the research philosophy and approach is followed by the research strategy and methods of applied data collection. Thereafter, a presentation of the literature review, a further description of the data collection and the data analysis is outlined. Finally, the research quality is discussed followed by the ethical considerations of the thesis.

2.1 Research philosophy and approach

With a perspective that derives from a pragmatic research philosophy, it was recognised that there are different explanations of the world that cannot be fully interpreted by an individual outlook. Hence, several realities may prevail to provide a complete picture of the systems (Saunders et al., 2016).

According to Hyde (2000), knowledge-creation is often obtained through different approaches to reasoning that ultimately result in a new understanding of a specific phenomenon. In the pursuit of a logical resolution that provides a systematic explanation of given presumptions, the deductive approach to reasoning is generally adopted (Spens and Kovács, 2006). By establishing a theoretical context, in which specific hypotheses or assumptions are elaborated to be further confirmed or proved incorrect by the empirical investigations, revision of existing theories can be achieved (Bryman and Bell, 2015). In this study, a deductive approach was deemed appropriate since the purpose of the thesis was to identify barriers that may exist towards the compliance of the regulatory security framework.

2.2 Research strategy and methodology

In the pursuit of achieving the purpose of this study, the reader was to be provided with valuable and reliable knowledge, based on the empirical findings and discussions revealed. In return, this emphasised the need for a well-structured and coherent presentation of the result and analysis, that could be explicitly interpreted by peers. In this respect, a research strategy should facilitate in the process of conducting research and contribute to the development of conclusions that eventually provides an answer to the stated research questions (Johannesson and Perjons, 2014). Thus, the use of a case study as the research strategy could, according to Yin (2014) provide a profound and comprehensive understanding about a phenomenon and its context. Furthermore, an explanatory case study could be used in the attempt to identify the cause and effect relationship of specific circumstances and why it prevails in different contexts (Johannesson and Perjons, 2014). In this thesis an embedded case study was used to allow for several units of analysis (Yin, 2014), namely knowledge-creation and information-sharing.

Additionally, the empirical data collection is an essential part of any explanatory case study (Yin, 2014). Accordingly, this advocates for an appropriate methodology that facilitates the process of recognising and collecting the relevant and crucial data. Hence, in scientific research, data collection techniques are usually categorised into two sub-groups, specified as qualitative and quantitative methodologies (Ketokivi and Choi, 2014).

A single method approach is the most common practice within any scientific research, Johannesson and Perjons (2014) suggest a constructive study process could be developed by applying two techniques of data collection. In addition, Bryman and Bell (2015) argue that a mixed-method approach allows for triangulation, the use of two or more methodologies. Findings collected by one methodology could then be cross-verified using a second method. This to provide both confidence and consistency in the data collected. The mixed-method approach using both quantitative and qualitative data collection method was found most suitable for this study, as it allowed for the investigated phenomenon to be further developed. Additionally, an increased understanding of the given assumptions in the study could be reached.

2.3 Literature review

In accordance with the deductive approach, a theoretical framework based on literature of peer reviewed articles was constructed. The literature review was done by using published literature as recommended by Bryman and Bell (2015). Various databases including Elsevier, Emerald, ScienceDirect, EuroLex and Summon Chalmers, were all used in order to find scientific journals, books and referencing-material. According to Bryman and Bell (2015) the use of specific key words, significant to the area of study, can facilitate in the process of identifying useful information. This strategy was therefore applied and different combinations of selected key-words were used to narrow down the scope and limit the search results. Examples of keyword that were used are; *maritime and port security; port organisations; regulatory compliance; regulatory security framework*. In addition, published reports from both governmental and non-governmental organisations were utilized together with articles and journals. As the International Ship and Port Facility (ISPS) Code entered into force in 2004 (International Maritime Organization, n.d.), literature published prior to then were used sparingly, since it was reasoned to have little relevance towards the study. In figure 1 below, the process diagram for the literature review is presented followed by table 1 that clarifies the initial and final phase of journal articles selected for the literature review.

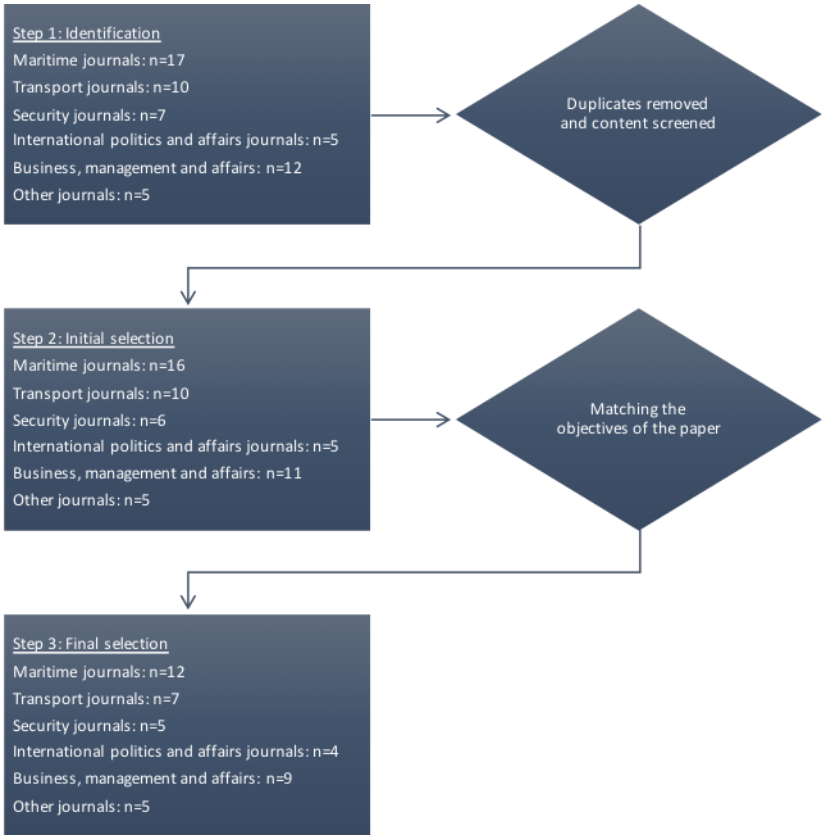

Figure 1: Process diagram for the literature review (Cole and Winberg, 2018)

Table 1: Overview of papers from selected journals in the literature review

Journal category	Journal	Number of papers in initial selection	Number of papers in final selection
Maritime Studies	*The Asia journal of shipping & logistics*	1	0
	Marine Policy	2	2
	Maritime Economics & Logistics	4	3
	Maritime Policy & Management	7	4
	Maritime safety & environmental administration	1	1
	WMU Journal of Maritime Affairs	2	2
Transport	*International Journal of Physical Distribution & Logistics Management*	1	0
	Journal of Transportation Security	4	4
	Supply Chain Management: An International Journal	1	0
	Transport Policy	1	1
	Transportation Research	2	1
	World Review of Intermodal Transportation Research	1	1
Security	*International Journal of Critical Infrastructure Protection*	2	1
	Journal of Homeland Security and Emergency Management	1	1
	Journal of Information Privacy & Security	1	0
	Security Journal	3	3
International politics and affairs	*American Political Science Review*	1	1
	Asia & the Pacific Policy Studies	1	0
	The British Journal of Politics and International Relations	1	1
	Policing & Society	2	2
Business, management & organisation	*Academy of Management Executive*	1	1
	African Journal of Economic and Management	1	1
	Annals of Operations Research	1	0
	Competitiveness Review: An International Business Journal	1	1
	European Journal of Innovation Management	1	1
	European Journal of Training and Development	1	0
	Human Resource Development Quarterly	1	1
	Journal of Knowledge Management	1	1
	Journal of International Management	1	0
	Journal of World Business	1	1
	Organization Studies in Higher Education	1	1
	Organizational Science	1	1
Other	*Ethnography*	1	1
	Implementation science	1	1
	Journal of Public Administration Research and Theory	1	1
	Public Administration & Development	1	1
	Public Administration Review	1	1
Total		**56**	**42**

2.4 Case study

To increase the quality of a case study, a broad range of sources are desirable (Yin, 2014). According to Yin (2014) there are six possible sources of evidence; *documents*, *archive records*, *interviews*, *direct observation*, *participant-observation* and *physical artefacts*. In this study, three bases for the theoretical and empirical data were used, surveys, interviews and a theoretical framework.

Primary data is data that is collected by the authors in order to achieve the purpose of the research. Secondary data is data collect by other persons than the researchers conducting the study (Bryman and Bell, 2015). In this thesis only primary data was used.

2.4.1 Survey

The application of surveys, is a research methodology that has the potential to facilitate in the process of gathering information from a large number of individuals within a short period of time (Johannesson and Perjons, 2014). According to Bryman and Bell (2015), a quantitative approach using surveys allow for the mass accumulating of information concerning the field of study. In this research a web-based questionnaire using Google Forms was used to collect the quantitative data. The survey was sent to persons actively working with security in Swedish ports. The data collected from the surveys was used as a source of evidence in the analysis.

Commonly, two different structures of survey questions are used, open-ended or closed-ended (Johannesson and Perjons, 2014). Closed-ended questions are claimed by Bryman and Bell (2015) to provide several benefits for the researcher, as they facilitate in the progression of *comparing* and *processing* answers from the survey. Moreover, from the perspective of the respondents, the closed-ended question approach allows for quick and easy responses, and usually provides a clearer understanding of the question at hand (Bryman and Bell, 2015). The survey used in this thesis was divided into four parts. The first part consisted of six questions that considered the respondent and the port at which they were employed. The second part of the questionnaire contained five closed-ended questioned with a one to five scale of not agreeing to fully agreeing. The third part had four closed-ended questions with a yes and no option. The final part consisted of one open-ended question. Using a web-based questionnaire was considered most appropriate, due to time efficiency and reducing potential mistakes (Bryman and Bell, 2015). The survey is viewed in Appendix I.

However, using a survey as a method of data collection also yields some disadvantages (Kelley et al., 2003). The pre-formulated options of response can increase the risks for partiality from the researchers as they decide on what answers are available (Johannesson and Perjons, 2014). Furthermore, it is not with absolute certainty that the desired response rate of the surveys can be obtained, since the respondents have the possibility to disregard the survey (Kelley et al., 2003). Nevertheless, the many advantages of using a survey as a data collection, and the inexpensive efforts needed for distributing the survey, were deemed as overweighing the negatives.

2.4.2 Interviews

In case studies, a research methodology that can be effective when wanting to gather both complex and profound information is interviews (Yin, 2014). Stemming from the qualitative methodologies, interviews can facilitate the process of collecting comprehensive and valuable knowledge about a specific subject area. Subsequently, the respondents' personal attitudes, opinions, emotions and experiences, may be observed to a greater extent (Johannesson and Perjons, 2014). In total, five interviews were conducted. Three of the interviewees were special adviser within maritime security, one interviewee was a lawyer, specialised in maritime transport and transport security law and lastly, one interview was with the Swedish Transport Agency (TSA). See table 2 below.

Table 2: Participating interview respondents

Abbreviation	Description of Respondent
SA1	PhD. and Special Adviser within Maritime Security
SA2	PhD. Professor Supply Chain Security and Special Adviser within Logistic Security
SA3	Special Adviser within Maritime Security
LE	Legal Expert, Lawyer, Special Adviser within transport and transport security law
STA	Representative from the Swedish Transport Agency

Furthermore, an interview can be structured and conducted in different ways (Kvale, 2007). In scientific research, it is frequently recognised that there are three classes of interviews; *structured*, *semi-structured* and *unstructured*, where the unstructured and semi-structured interviews are preferably chosen when studying complex topics (Harrell and Bradley, 2009). Further, it can be argued that a semi-structured interview allows the respondents to present their attitudes and opinions freely, unobstructed by a predetermined set of options of response, which normally applies for the structured approach (Kvale, 2007). For the interviews conducted herein, a semi-structured approach was considered to be the most suitable alternative. The semi-structured approach is established around a set of predefined questions, however, Johannesson and Perjons (2014) claim that the interview process allows for a high level of flexibility due to the open-ended structure of the questions. Furthermore, this can provide an incitement for the discussion to be further elaborated as the interview proceeds and can lead to new and valuable knowledge towards the research topic (Kvale and Brinkmann, 2009).

However, it is important to be aware of the disadvantages when applying interviews as a data collection approach (Yin, 2014). For instance, the long period of time needed for conducting the interviews, transcribing them and analysing the collected data can be viewed as large drawbacks (Johannesson and Perjons, 2014). It is also regarded as a weakness of interviews as a data collection method that a risk for bias questions arises and that the respondents express to the interviewers what they wish to hear instead of their own opinion (Yin, 2014). Furthermore, the analysis has to be permitted to take

time; this to allow for personal reflection and weighing in on aspects that may have influenced the results of the conducted interviews (Johannesson and Perjons, 2014).

Moreover, as far as practically possible, the interviews were conducted face-to-face with the respondents. According to Opdenakker (2006), conducting a face-to-face interview can provide valuable information that otherwise would not be attained using other techniques such as telecommunication. Face-to-face meetings provide an opportunity to add valuable extra dimensions such as to observe and respond to the interviewee's body-language, i.e. if there are any concerns with understanding a question or if the respondent feels uncomfortable with the situation (Bryman and Bell, 2015). However, in some instances face-to-face interviews were not possible due to time and geographical location. In those cases, Skype and telephone was used for conducting the interviews.

Furthermore, in order to increase the degree of confidence in the discussions and increase the possibilities to attain valuable and sensitive information, all the interviews were conducted in the individuals' native language, which in all instances was Swedish. In addition, all the interviews were performed in neutral and private environments. According to Johannesson and Perjons (2014) the location of the interview could be the difference towards the respondents willingness to expose sensitive information or not. This is confirmed by Bryman and Bell (2015) who similarly argue that the selection of a private venue shall be considered to further limit or exclude the possibilities of someone overhearing sensitive information shared during the meeting.

Prior to the interviews commenced, the consent of the respondent to partake in the study at their own free will was confirmed. The respondents were also asked if the interviews could be recorded, if not, only notes were taken. Furthermore, the respondents were informed that they had the right to stop the interview at any given time if they wished and that their anonymity would be kept throughout the study and also upon its completion. The interviews lasted for thirty to seventy minutes, averaging about forty-five minutes. The two semi-structured interview templates are viewed in Appendix II and Appendix III.

2.5 Participating port organisations

The ports were divided into two main groups with respective sub-groups. The first main group was the size of the ports, i.e. *large*, *medium* and *small*. This categorisation was based on statistics retrieved from Trafikanalys (2017). A *small* maritime port in this research is defined as a port that handles less than two million tonnes of cargo, a *medium* port handling two to five million tonnes and a *large* port handling five million tonnes or above. A second categorisation of ports was based on a report from (Sveriges Hamnar, 2016). This was used to identify what ports in Sweden handle passengers. In Sweden, the eight largest passenger ports handled 93,5 percent of all passengers during 2016 (Sveriges Hamnar, 2016). The eight ports identified were classified as passenger ports and the remaining ports were categorised as non-passenger ports.

Moreover, the respondents to the surveys were security responsible personnel at maritime ports in Sweden. The ports selected came from the Swedish Maritime Administrations list of all public ports in Sweden (SJÖFS 2013:4). According to SJÖFS

2013:4, there are a total of 54 public ports in Sweden. However, seven ports were not asked to participate in the study since they do not facilitate vessels large enough to be compelled to comply to all the maritime and port security regulations reviewed. Two additional ports were not asked to participate since they today are fully operated by private companies. Furthermore, a total of six port organisations operate more than one port. In total, these six port organisations operate 17 ports. As a result, a total of 34 port organisations were asked to participate in the study. The initial contact was made via email where the project was introduced and the respondent encouraged to involve the port and contribute to the survey. The email also contained the research ethics of the study and a link to the web-based survey. If the port organisations had not responded to the survey within a week, a telephone call was made to ask if they wished to partake. Out of the 34 asked port organisations, 16 (47 percent) agreed to partake and answered the survey before the set deadline. One port organisation chose to be anonymous when conducting the survey and could therefore not be sorted according to size and type of cargo handled. Subsequently, figures in the Result and Analysis chapter where port organisations are categorised by the stated variables only illustrates the answerers from the remaining 15 port organisations.

2.6 Data analysis

Data requires preparation, analysis, interpretation and presentation for conclusions to be drawn from it (Johannesson and Perjons, 2014). In accordance with Bryman and Bell (2015), the data analysis process commenced whilst the data collection was ongoing. This iterative process is common practice when the research is focused on qualitative data. Mutually, nominal, ratio and ordinal data was collected from the survey.

Throughout the process of the interviews, minutes of the meetings were taken to allow for a summarisation to be drawn up after each occasion. Further, the summarisation facilitated deductive analysis to take place, i.e. specific statements or instances could form a general statement as more and more data was collected (Denscombe, 2014). The summarisation of each interview was then sent back to the respondent in order to allow for potential errors to be eradicated. The research was conducted as an explanatory single case study with embedded analysis, implicating that there was more than one unit of analysis (Yin, 2014).

2.7 Research quality

Several models have been developed for assuring quality of research (Yin, 2014, Bryman and Bell, 2015, Easterby-Smith et al., 2015, Saunders et al., 2016). For example, Easterby-Smith et al. (2015) have presented a model to ensure robust research, containing three elements; *reliability*, *validity* and *generalisability*. However, this model is recognised to be best suited for quantitative studies. In contrast, the Bryman and Bell (2015) model is recognised to be more applicable for qualitative studies. This model includes five elements or criteria; *credibility*, *transferability*, *dependability*, *conformability* and *authenticity*. Nonetheless, even if both the named models have been examined, the primary source used in this thesis to assess the quality of the research derives from the social scientist Yin (2014). Four tests have been developed by Yin (2014) to ensure the quality of an empirical social research, where one category is case studies. It was therefore deemed as the most appropriate model for the study at hand.

Firstly, Yin's model tests for the *construct validity* of the research (Yin, 2014). This can be achieved by using three tactics; the chain of evidence, the use of key informants for review and the application of multiple sources of evidence. In this research, multiple sources of evidence were used during the conducting of this thesis. Initially, published research was studied to recognise already identified barriers. These barriers were then used as a support to formulate the survey. The received answers from the respondents of the survey were subsequently used to formulate an interview template. Furthermore, experts, such as a lawyer, a maritime education expert and a supply chain security expert, were asked to review certain parts of relevant material to confirm additional validity.

The second test according to Yin (2014) is *internal validity*. This could be compared to Bryman and Bell's (2015) *credibility*, where triangulation is fundamental. Triangulation in the field of social science is when several sources are used to gather data. To ensure *internal validity* herein, a conclusion was only drawn when several sources indicated towards the same bearing. Further, the *internal validity* was established by recording all but one interview that were conducted. Furthermore, the translated citations used in the thesis were all sent back to the respondents for review. As a result, this minimised the risk of misinterpretations.

The third step for quality research is *external reliability* (Yin, 2014). An *external reliability* is achieved when making the research applicable in other circumstances (Bryman and Bell, 2015). This is in accordance with the third step of Easterby-Smith et al. (2015) to achieve robustness, *generalisability*. The framework of the thesis and the participating maritime ports were limited to Sweden. However, the model that was applied could be used to research the ports that did not wish to partake and to study port organisations in other countries and across the globe.

Finally, Yin (2014) suggests testing the *research reliability*. *Research reliability* allots to minimising any prejudices or mistakes (Yin, 2014). Thus, a reliable study should be replicable by other researchers and the same result should be achieved (Easterby-Smith et al., 2015). In alignment with this, Bryman and Bell (2015) state *conformability* as a criteria. They advise objectiveness and not to allow for personal values or beliefs to interfere with the research. Furthermore, Bryman and Bell (2015) also address *dependability* as a criteria for research quality, where the concern is the openness of the researchers during the process and progression. It should be possible for a peer to follow the entire course of the study, which is in alignment with the proposals made by Yin (2014) who recommends a case study database. During the course of the study, OneDrive was used to gather all information in one place. This was used to allow for the entire process to be mapped. Additionally, a day-to-day log was kept throughout the course of the study. The log detailed all the decisions that were made and meetings that were held. The minutes from all meetings were compiled in one file together with the notes of all material gathered.

2.8 Ethical considerations

Bryman and Bell (2015) state that research ethics contains four main elements that should be regarded; *invasion of privacy*, *lack of informed consent*, *deception* and *harm to participants*. Since certain data collection in the project could be viewed as sensitive,

all the research was conducted in accordance with The European Code of Conduct for Research Integrity (ECCRI). This required that the research project always aimed to be honest in its communications and reporting, objective, fair in providing references, impartial and as reliable as practicably possible (The European code of conduct for research intregrity, 2017) . All the data collected was also handled according to ECCRI guidelines. The data collected was used for the sole purpose of the research project at hand. All the participants of the research, as well as the data collected from the subjects, were kept anonymous. Further, for collecting primary data, all the questions asked and answered in the survey and during the interviews, were conducted in a manner as to not jeopardise the anonymity of the survey participants. The authors of the research take full responsibility for the data collected and research published (The European code of conduct for research intregrity, 2017).

3 FRAME OF REFERENCE

This chapter covers a deeper review of the published research, theories and concepts, and how they can be applied to the potential barriers in order to comply with the regulatory security framework. It also highlights identified gaps in previous studies and presents probable barriers recognised by scholars in the field.

3.1 An overview of maritime and port security

The following section provides an introduction to the historical context of maritime and port security and while delivering a description of the present and future concerns within the sector. Furthermore, it observes and comments on definitions in the area of safety, security and threats. Additionally, definitions of ports and port facilities are outlined.

3.1.1 Historical development of maritime and port security

Maritime security has been an integral part of the global maritime industry ever since the middle of the 15th century (Eklöf Amirell, 2016). This may be substantiated by the introduction of the papal decree of Pope Nicholas V in 1455, entitled the *Bull Romanus Pontifex*, *w*hich is widely believed to be the first ever documented security regime (Eklöf Amirell, 2016). Despite that the threats opposed by the industry historically appear dissimilar to the circumstances in the modern world, the objectives of the very first documented security regime much resembles those that are in place today. Historically, the maritime security regimes' purposes were to increase international order and security at sea by prescribing statutory regulations (Eklöf Amirell, 2016). Despite the fact that maritime security during the past 500 years has been a huge concern to the maritime domain, and the world's trading of goods at sea (Eklöf Amirell, 2016), maritime security as a field of research has not been subject to increased academic interest until some three decades ago (Germond, 2015).

Furthermore, the situation of modern global maritime security conditions is mainly the result of developments and events that have taken place from the 1980's until the present day (Eklöf Amirell, 2016). Significant here, is the introduction of the 1982 United Nations Convention of the Law of the Sea (UNCLOS) where limitations were set to the individual states' obligations for sustaining global maritime security (Eklöf Amirell, 2016). Here, the introduction of Exclusive Economic Zones (EEZ) achieved a further extension of the territorial waters to 200 nautical miles from the Sovereign State baseline. Individual States could then give priority to maritime security within their own EEZ, as they were given jurisdiction over set parts of the seas and oceans (Edgerton, 2013). Additionally, the hijacking of the Italian cruise ship *Achille Lauro w*as the first maritime incident grounded on political incitements. This occurrence together with several hijackings of aircrafts during the same time period gave rise to new global security concerns, not only for the maritime industry but for security in general. Thus, a necessitation for actions and countermeasures to tackle new threats opposed by the industry had been born (Wengelin, 2012).

Moreover, within the maritime transportation sector, the correspondence between security and management has been of great significance for organisations in order to preserve their daily operations and the continuous development of their businesses (Thai, 2007). Thus, to ensure safe and secure transportation of passengers, crew and

goods has been a constant responsibility and concern to managers within port and vessel operations. However, security has been regarded more as a set of standard processes and procedures necessary by organisations to sustain a minimum requirement for safe operations (Kenneth, 2015). Due to this, it was not until 2001, in the aftermath of the 9/11 terrorist attacks, that the perception of security became the subject for a comprehensive transformation (Andritsos and Mosconi, 2011). The new and significant threats opposed by the industry after the war on terror had been declared by the USA and their allies in 2001 hence resulted in increased considerations on how security for the maritime transportation system was to be efficiently operated and managed (Helmick, 2008, Kenneth, 2015).

As a response of the 9/11 attacks, the International Ship and Port Facility Security (ISPS) Code was developed by the International Maritime Organization (IMO) to limit the risk of terrorist attacks from happening in the future (Malcolm, 2016). In July of 2004, the ISPS Code entered into force just 18 months after its adoption, while the new maritime regulatory security framework was adopted into the International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended, (chapter XI-2 on Special Measures to enhance Maritime Safety) on 1 July 2004, thus making it fully mandatory to comply with. Not only was the ISPS Code regarded to be a new and comprehensive mandatory security regime, but its introduction significantly changed the way the maritime industry perceived and worked with security related issues (Kenneth, 2015).

3.1.2 Present and future concerns

According to Bueger (2015) and Germond (2015) maritime security is the latest buzzword within international relations and especially within the maritime domain. Hence, this implies that major actors are including the topic of maritime security in their mandate and wish to influence its direction. Consequently, political leaders managing governmental instruments with the intention to enhance security, such as regulations, are subject to pressure from both commercial and public interests (Edgerton, 2013). Similarly, the regulations that have been put into force were done at such a speed that most stakeholders were not asked to contribute in making the regulations feasible or compelling (Papa, 2013).

Moreover, according to Edgerton (2013) maritime security is regarded as an important issue that is essential to manage and organise in an efficient manner. However, organisations tend to focus on the drawbacks of security management rather than the positives. Edgerton (2013) has identified three common concerns towards maritime security; [1] *costs for implementation of security measures*; [2] *increased governmental control and supervision;* and; [3] *the risk for inefficient and inflexible supply chain operations*. These common concerns are considered in the following paragraphs.

Firstly, in a dynamic market characterised by intense and international competition, it is important for organisations to efficiently administer their financial resources and increase their profits. However, security management is, in some cases, regarded as an economic burden to the organisations (Edgerton, 2013). According to Mazaheri and Ekwall (2009) this is a prominent concern within the maritime port sector, particularly when smaller ports are to a greater extent than larger ports affected by the implementation costs of security measures in order to comply with the regulations

stipulated. Here it is believed by Burns (2013) and Mileski et al. (2015) that the financial investments required for implementing security measures in order to comply with the security regulations are not deemed as justifiable from an economic point of view.

Secondly, there is a certain level of reluctance to the increased supervision and control from governmental bodies, implied by the processes required to comply with governmental regulations. According to Edgerton (2013) maritime organisations in general, and ports in particular, have a negative attitude towards the processes and procedures necessary to facilitate compliance with the security regulations. There is often suspicion from organisations when new initiatives are introduced that exhaust resources before it has proven to have an effective outcome (SafeSeas, 2018). Audits and inspections are a natural part of compliance, but necessitate human-resources that are required to shift focus from their usual responsibilities (Edgerton, 2013).

Thirdly, Edgerton (2013) states that in order to remain competitive within the dynamic environment of the shipping industry, there is an urging need for organisations to preserve efficient and flexible supply chain operations (Mileski et al., 2015). According to Thai (2007) increased and stringent security measures could have a negative impact on the efficiency of maritime operations and the ability to deliver and preserve Just-In-Time deliverance. Thus, instead of investing in the development and successful implementation of security management, organisations tend to maintain maritime and port security measures at the least level possible, with the focus on cost-efficiency in order to comply with the regulations (Edgerton, 2013).

In addition, it is widely recognised that public opinion effects policy-making more than policy-making effects the public opinion (Page and Shapiro, 1983). This phenomenon is apparent within the maritime industry (Edgerton, 2013). Even though, the public lacks in both knowledge and understanding of maritime operations and maritime security, legislators and policy makers feel pressed to act upon the demands to satisfy the public interest (Metaparti, 2010). Due to this, assertive security measures are implemented regardless of their actual efficiency and effectiveness. Political leaders wish to create an impression, that is easy for the public to recognise, of a strong and reliable government with the ability to act upon emerging threats, i.e. terrorism (Metaparti, 2010, Edgerton, 2013).

However, despite that maritime security today is deeply influenced by both commercial and public interests (Edgerton, 2013), its future and successful development is highly dependent on additional factors. For instance, Roe (2009) argues that policy makers constituting maritime governance, through the IMO, the European Commission (EC) and State governments, face challenges to sufficiently and effectively manage maritime security. Roe (2009) continues to state that the current jurisdictional framework and the maritime policies that have emerged during the twentieth century, are in many ways inadequate, ineffective and imperfect. In a new and globalised world, where flexibility and efficiency play vital parts of the commercial structures in the market, they are rapidly becoming obsolete (Roe, 2013). As Wengelin (2006, p. 10) states, "*rules and regulations do not travel well over time and space*".

Global maritime governance is greatly dominated and impacted by Sovereign States' vested interest and agenda (Roe, 2013). Authorities consisting of inter-governmental institutions and collaborations, such as the IMO and the EC, with the intention to enact on improved global maritime policies and regulations, appear to have little relevance in this context (Roe, 2013). Furthermore, influences from commercial groups within the domestic maritime markets may force the national governments to implement favourable policies and legislations. Consequently, international negotiations with the intention to improve global maritime policies and regulations have been subject to the nation state's incitements of satisfying domestic interests (Farrell, 2001, Roe, 2009).

As a result of the above stated influencing of policy making from commercial actors, Roe (2013) argues that an imbalance, where the societal interests (i.e. security, safety and environment) has been given a lower priority for the benefit of business interests. Furthermore, the State-shipping relationship can be argued to have had a negative impact on both national and international maritime governance. This enables the shipping industry to seize the opportunity and take advantages of policy failures in order to promote its own commercial interests (Roe, 2013).

3.1.3 A conceptualisation of safety, security and threats

In order to fully comprehend and evaluate maritime security, some considerations are required with regards to the concept of security and its signification. Misperceptions exist concerning the meaning and disparity between the words safety and security (Andritsos and Mosconi, 2011). The words are often used within the same or similar contexts, hence resulting in an inaccurate utilisation. In certain languages, there is even a lack of terminology that distinguishes between the meaning of safety and security (Andritsos, 2013). These languages possess only one word describing them both, Swedish being an example. Furthermore, the words could differ significantly in their interpretation depending on the context in which they are used (Piétre-Cambacédès and Chaudet, 2010). For instance, Bueger (2015) argues that a debate and reasoning around the term maritime security and its definition would allow for the sector to chart what disputes exist around its context, and thence show where the improvements should be focused. A clarification and definition of both safety and security in the maritime context is presented below.

Safety and security have been defined by Andritsos and Mosconi (2011). Their definition for safety is as follows:

> *"The state of being free of risk or danger (natural or man-made, accidental or intentional); when used as an attribute, it encompasses all measures, actions or systems aiming at ensuring the state of safety." (Andritsos and Mosconi, 2011 p. 2)*

The concept of maritime safety covers a broad set of aspects, thus its definition is not entirely explicit, but tends to be implicit in many situations. Within IMO, the most senior technical body for safety-related matters is delegated to the Maritime Safety Committee (MSC), a body that is regulated in Article 28(a) of the original IMO Convention of 1948. The current MSC is supported by seven sub-committees; *Carriage of Cargoes and Containers*; *Ship Design and Construction*; *Implementation of IMO*

Instruments; *Navigation, Communications and Search and Rescue*; *Human Element, Training and Watchkeeping*; *Ship Systems and Equipment;* and; *Pollution Prevention and Response* (International Maritime Organization, 2018a). Each of these bodies comprise IMO's (173) Member States, Governmental Organisations and Non-Governmental Organisations and are collectively tasked to consider and resolve the vast and various number of challenges that embrace "maritime safety".

Furthermore, security has been more clearly defined by several organisations in their preambles to security regulations. However, for clarity the definition used by Andritsos and Mosconi (2011) is stated here:

> *"The set of means/ actions through which safety is ensured, in particular against intentional threats; it encompasses all measures, actions or systems aiming at preventing intentional threats from compromising safety." (Andritsos and Mosconi, 2011 p. 2)*

This definition is much aligned with the definition of maritime security provided by the Regulation (EC) 725/2004 on enhancing ship and port security:

> "*… maritime security means the combination of preventive measures intended to protect shipping and port facilities against threats of intentional unlawful acts" (Regulation EC 725/2004, Article 2)*

The definition stated by Andritsos and Mosconi (2011), provides a concept for security in general, while the definition in the Regulation incorporates the perception of security into the context of the maritime domain. Commonly, security could be regarded as the proactive and protective actions or countermeasures taken against unlawful acts, with the intention to cause any harm on assets, tangible or in-tangible (Regulation EC 725/2004, Andritsos and Mosconi, 2011).

Furthermore, the United Nations (UN) Secretary-General report recognised that there is no universal definition of maritime security. Instead, the report documented seven exclusive threats to maritime security; [1] *piracy and armed robbery*; [2] *terrorist acts*; [3] *the illicit trafficking in arms and weapons of mass destruction*; [4] *the illicit trafficking in narcotics*; [5] s*muggling and trafficking of persons by sea*; [6] *illegal, unreported and unregulated fishing;* and; [7] *intentional and unlawful damage to the marine environment* (United Nations, 2008).

Moreover, a threat is often used interchangeably to terms such as vulnerability and risk. However, threat is an act or actor that could damage or harm a person, property, organisation or State. The key words in the definition of threat are that of act or actor, which denotes that an action, or a potential action, stands behind the term (Edgerton, 2013). The definition of threat is purely negative compared to the definition of risk, that describes an uncertainty of outcome. Even though risk is often associated with negative consequences this is not always the case, as risk could be regarded as an opportunity that eventuates into a positive result (Hopkin, 2014).

3.1.4 Defining a port and port facility

A port can be defined in several ways and be applied to several categories of entities. However, sea ports have a number of essential mutual functions. These functions include moving freight and/or passengers across the sea/shore interfaces as well as servicing maritime vessels (Andritsos, 2013). Furthermore, there are differences between port facilities and ports. According to the EC, for example, a port facility is defined as:

> *"…a location where the ship/port interface takes place; this includes areas such as anchorages, waiting berths and approaches from seaward, as appropriate" (Regulation EC 725/2004, Article 2:11)*

However, a port is defined by the EC as:

> *"…any specified area of land and water, with boundaries defined by the Member State in which the port is situated, containing works and equipment designed to facilitate commercial maritime transport operations" (Directive 2005/65/EC, Article 3:1)*

Furthermore, in this thesis the terms "*port*" and "*port facility*" are used to describe public commercial ports and port facilities, unless otherwise stated.

3.2 The regulatory framework for maritime and port security

Regulatory security frameworks for maritime ports and port facilities exist on the global, international and national level. In this thesis, the global level refers to the IMO amendments to the 1974 SOLAS Convention, viz. the ISPS Code. The international level refers to the European Union (EU) and the EC regulatory framework. Further, since this thesis focuses on Swedish ports, the national level focusses on the acts, ordinances and regulations of Sweden deriving from the global and international level. Furthermore, other regions and countries have their own regulations, however this thesis only deliberates regulations affecting Sweden.

In the following section a description of the legal instruments on each level is presented based on *the governing body*; *a brief history of implementation*; *an overview of the legal instruments;* and; *responsibilities of ports* will be highlighted. The presentation of the legal frameworks aims to clarify what port facilities and ports are obliged to work towards and to simplify the analysis and discussion of the result of potential barriers towards compliance.

3.2.1 The global level

The ISPS Code entered into force in 2004 under SOLAS, 1974, as amended, and has since formed an international mandatory security system for shipping (International Maritime Organization, 2017). The Code was a direct result of the 9/11 attacks on the World Trade Centre in New York and the following years attacks on the tanker *M/V Limburg* and the *USS Cole*. Prior to the adoption of the ISPS Code, the adoption of Resolution A.924(22) took place in November 2001 and was the first attempt to increase global maritime security after the 9/11 attacks. The Resolution aimed to mitigate threat by revising the existing security regulations and in turn lead to the

adopted amendments to SOLAS, 1974, as amended, namely the ISPS Code. Being the fastest implemented Code in IMO's history, the amendments were headed by the United States Coast Guard (USCG) calling for a swift and prompt measure to be put in place to further prevent security threats towards ports and vessels across the globe. Strong rhetoric and lobbying, mainly from the USCG, by means of exploiting fear of great economic concern in relation to terrorism, enabled the great speed of events (Metaparti, 2010). The rare swiftness of the ISPS Code's adoption can be recognised when viewing the time frame for previous adoptions of amendments, which on average is approximately ten years (International Maritime Organization, 2018b).

Henceforth, the initial catalyst of what was to evolve into the ISPS Code had its start in 1986 after the *Achille Lauro* seizure when the Italian cruise ship was hijacked by terrorists from the Palestine Liberation Front. One passenger was shot and killed during the two-day drama. Since the hijacking was a significant actual terrorist act, the IMO felt the urge to respond without delay and thus adopted Resolution A.584 (International Maritime Organization, 1988). Further, the UN General Assembly necessitated a study focusing on terrorist threats towards shipping. The study resulted in recommendations that were adopted at the IMO as measures to prevent unlawful acts against crew and passengers, MSC/Circ. 443. The circular laid the foundation for what would advance to become the ISPS Code some fifteen years later (International Maritime Organization, 2018b).

In figure 2 below, the vital period of events that gave rise to the development and adoption of the ISPS Code are illustrated. Moreover, the cause-effect relationships are explained. In figure 2, "the causes" are the events and political pressures leading to the adoption of the resolutions, signified as "the effects".

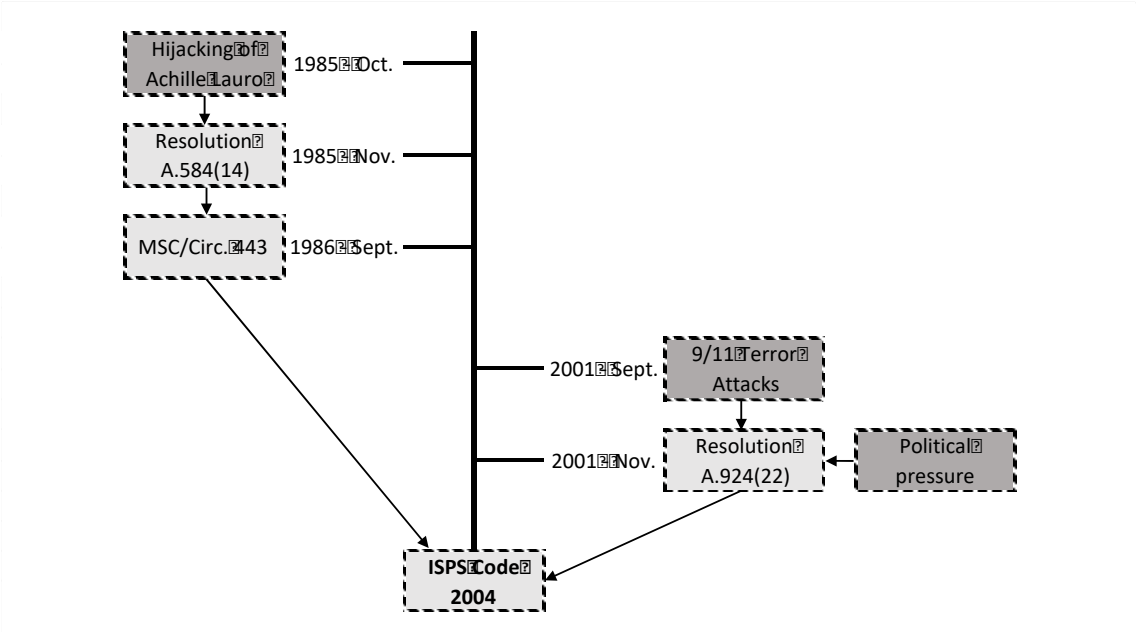

Figure 2: The critical period of events that gave rise to the adoption of the ISPS Code (Cole and Winberg, 2018)

The background and history of the ISPS Code shows how it was introduced and what threats and powers ensured its rapid passage through the legal framework through to its

entry into force. However, the actual threat that the ISPS Code should mitigate is not defined in the Code, since it is clear it stems from a fear of terrorist actions (Wengelin, 2012). In the ISPS Code, the objectives are outlined as; *to detect security threats and implement security measures; to establish roles and responsibilities concerning maritime security for governments; local administrations; ship and port industries at the national and international level*; *to collate and promulgate security-related information*; *to provide a methodology for security assessments so as to have in place plans;* and*; procedures to react to changing security levels (International Maritime Organization, 2003)*. As stated by Trelawny (2005);

> *"The purpose of the ISPS Code is to provide a standardized, consistent framework for evaluating risk, enabling governments to offset changes in threat levels with changes in vulnerability for ships and port facilities." (Trelawny, 2005, p. 4)*

Furthermore, the ISPS Code is not applicable to ports, but rather to port facilities. In addition, it is not applicable to all ships and port facilities. It applies only to cargo ships of 500 gross tonnage and upwards engaged on international voyages, passenger ships engaged on international voyages, mobile offshore drilling units and port facilities serving the before stated ships (International Maritime Organization, 2003).

Moreover, the ISPS Code is divided into two parts. The first part (Part A) outlines mandatory provisions while the second part (Part B) outlines a set of guidelines on how to implement the security provisions stated in the first part (International Maritime Organization, 2017). More specifically, Part A specifies obligations by contracting governments, port facilities, ships and shipping companies. However, even though Part B is not mandatory, a failure to comply could be regarded as a failure to exercise due diligence (International Maritime Organization, 2003).

Further, three maritime security levels were introduced by the ISPS Code (International Maritime Organization, 2003). The normal operating level, Level 1, is to be used on a daily basis to ensure that the facility maintains a minimum required standard in terms of security. Level 2 is applied when a potential threat has been detected and Level 3 is only put in use when an incident has already taken place or reliable information is made available that there is a clear threat. If a ship is in port, it has to adopt the level of security of the port facility, or higher, if it itself is operating at a superior level (International Maritime Organization, 2003).

While the ISPS Code covers both ship and port facilities, the ports facilities are deemed particularly vulnerable to security threats since access can be gained from both the water- and shore side. Ports in most cases, consist of large areas with obscure, hidden places, such as warehouses, office buildings and docks. In addition, all port facilities that are covered by the ISPS Code must have a *Port Facility Security Officer* (PFSO) whom should have the ability to perform a security assessment, update and maintain the security plan and exercise all the necessary actions (International Maritime Organization, 2017). Moreover, all port facilities are required to have a *Port Facility Security Plan* (PFSP) formulated after a rigid risk analysis and approved by the National Authorities of the Member States (International Maritime Organization, 2003). The

foundation of the ISPS Code is the *Port Facility Security Assessment* (PFSA), an essential and integral part of the process of developing and updating the PFSP (Andritsos, 2013). The PFPS should be periodically reviewed by the Member State and updated if any major construction or changes are made in the port facility (International Maritime Organization, 2003).

Furthermore, IMO published the first edition of the Guide to Maritime Security in 2012. The publication aims to assist States in the "*implementation, verification, compliance with, and enforcement of, the provisions of the IMO maritime security measures*" (International Maritime Organization, 2018b) where among other measures the ISPS Code is the key.

3.2.2 The international level

In connection with the adoption of the ISPS Code, the EU initiated the process of developing a new regulation for maritime and port security, as a further extension to the global requirements and guidelines (European Commission, 2018a). The intention of developing an EU Regulation for maritime and port security was to establish a harmonised interpretation of the ISPS Code and develop a common regulatory framework applicable to the EU and its Member States (Transportföretagen, n.d., Papa, 2013). In March 2004, the EC implemented the additional maritime and port security regulation under the provision of Regulation (EC) 725/2004 on enhancing ship and port security. The regulation entered into force on the 1st of July 2004 with the implication that all EU Member States were obliged to comply with the then newly stipulated regulation (Regulation EC 725/2004). Subsequently, the EC Directive 2005/65/EC on enhancing port security was introduced as a complement to the Regulation. The Regulation and the Directive constitutes the EC's regulatory framework for the protection of maritime transportation and infrastructure against risks and threats by unlawful intentional acts (European Commission, 2018a).

Furthermore, an EC regulation, such as Regulation (EC) 725/2004, when implemented becomes an international legislative act that is mandatory and therefore must be adopted by all EU Member States. In addition, when the EC amends existing regulations EU Member States are required to amend their national laws accordingly (European Union, 2018). Moreover, an EC directive, such as the EC Directive 2005/65/EC, is also a compulsory legislative act with predefined objectives that all the Member States must accept. However, EC directives differ in terms of arrangement and implementation. In this particular case, each individual Member State has the freedom to institute and frame their own regulatory instruments provided that they abide with the objectives of the EC directive (European Union, 2018).

With the introduction of Regulation (EC) 725/2004, the ambition and intention of the EC was to increase the level of maritime and port security inside the borders of the EU. Improved security should be granted for vessels and ports through enhanced and more detailed regulations (Papa, 2013). Unlike the provisions stipulated under the ISPS Code, the EC incorporated certain elements of Part B of the Code into their own Regulation and made it mandatory to comply within the EU (European Commission, 2018a). The EC thus extended the regulatory security framework in order to assure that maritime security prevails at the highest level possible. Furthermore, the extension was made to

provide an uniformed understanding and implementation for all Member States (Papa, 2013). In addition, the regulation includes two other substantial supplements that have not been covered by the ISPS Code. Firstly, a further extension to the area of application has been added, with regards to the type of ship to be comprised by the Regulation. Secondly, the EC is given authorisation by the Regulation to undertake supervision and inspections; this to ensure that the Member States fulfil their obligations within the scope of the stipulated provisions (Regulation EC 725/2004, Swedish Riksdag, 2005).

In many aspects, Regulation (EC) 725/2004, focuses on maritime security for vessels and the port-ship interaction (Regulation EC 725/2004). However, there is a lack of measures that comprise the entire port area and transportation chain (Regulation EC 725/2004). According to Papa (2013) this could be advocated to result in an inadequate and ineffective security regime. Responding upon these issues, the EC developed and implemented the Directive 2005/65/EC on enhancing port security (Papa, 2013). The directive applies to all EU ports, in which one or more port facilities is/are located (Andritsos and Mosconi, 2011). Provided as a necessary supplement to the Regulation, its objective is to assure that the complete port area, not covered by the Regulation, is incorporated into the security regime. Thereby, the EC could provide a sufficient and effective regulatory framework for security, expedient in order to protect the entire maritime infrastructure and transportation chain (European Commission, 2018a).

3.2.3 The national level

Sweden is, as a Member State of both the IMO and EU, liable to comply with all the regulations for maritime and port security prescribed by each of the respective institutions (Swedish Transport Agency, n.d. a). In order to comply with the requirements of EC Regulation 725/2004 directly and indirectly with the ISPS Code, the Swedish Riksdag has developed and implemented Act (2004:487) on maritime security. Provided as a supplement to Act (2004:487), the Swedish Government has issued Ordinance (2004:283) on maritime security (Swedish Riksdag, 2005). In compliance with Act (2004:487) and Ordinance (2004:283), the Swedish Maritime Administration (SMA) has enacted the regulation on maritime security through SJÖFS 2004:13 (Swedish Transport Agency, n.d. a). Moreover, to achieve the objectives stipulated in EC Directive 2005/65/EC, the Swedish Riksdag and the Swedish Government has adopted Act (2006:1209) and Ordinance (2006:1213) on port security, respectively. Subsequently, the SMA has implemented regulation SJÖFS 2007:1 on port security (Swedish Transport Agency, n.d. a). Thus, the above presented acts, ordinances and regulations constitute the national regulatory framework for maritime and port security in Sweden.

Moreover, in order to clarify the Swedish judicial system for maritime and port security an explanation of the national legislative instruments is required. A Swedish act is a statutory instrument ratified by the Swedish Riksdag and is the most important constitution of the legal system for the nation. The content of an act has a general outline. In addition, the Swedish Riksdag is required to ratify adoptions to the Swedish constitution in accordance with EC regulations and directives (Swedish Riksdag, n.d.). Further, the Swedish Government stipulates ordinances that function as a more detailed complement to the acts. Finally, administrative authorities in Sweden institute

regulations within their corresponding field of responsibility. Hence, working as a supplement to both the act and ordinance, the Regulation provides the most detail and final provision (Notisum, n.d.).

In 2003, the Swedish judicial system initiated a fast-paced process of developing a regulatory framework in accordance with the stipulations of EC Regulation 725/2004. One year after the initiation the Swedish Riksdag, the Swedish Government and the Swedish Maritime Administration (SMA) completed the implementation phase of their respective systems of regulations (Swedish Riksdag, 2005). The content of each respective system of regulation will be briefly stated in the following paragraphs.

Firstly, Act (2004:487) is composed of different provisions, giving the nominated regulatory authority for maritime security the warranty to make decisions on; *reviewing of people and property; the appropriate security level to be applied for vessels and port facilities; penalties for not complying with or if violation of any sort occurs against the stipulations in the EC Regulation; etc.* (SFS 2004:487).

Secondly, stipulated in Ordinance (2004:283) the Swedish Transport Agency (STA) is designated as the nominated regulatory authority for maritime security in Sweden. In addition, it includes provisions that regulate the responsibility of different authorities (such as the Swedish Coast Guard, the Swedish Police Authority and Swedish Customs Agency) to aid and support the STA in the supervision and safeguarding of maritime security in Sweden (SFS 2004:283, SFS 2008:1152, Swedish Transport Agency, n.d. b).

Lastly, SJÖFS 2004:13 regulates issues such as; *maritime security assessments and plans; point of contact (Swedish Coast Guard) for advice, assistance and reporting to/from ships in regard to information/concerns of maritime security; declaration of security between the ship and port facility; IMO identification numbers for ships; record of history for Swedish ships in international trade; etc.* (SJÖFS 2004:13).

In the same way, as for Regulation 725/2004, the introduction of Directive 2005/65/EC in 2005 necessitated the development and implementation of a Swedish regulatory framework for port security. In order to conform with the objectives of the EC Directive, the Swedish Riksdag established Act (2006:1209). The stipulated provisions regulate issues concerning; *area of application with regard to ports and defining the port in accordance with the Directive; appropriate security levels to be applied for ports; review of people and property in connection to the port area; safeguarding requirements for ports; the representative for the port; etc.* (SFS 2006:1209). Additionally, the requirements in the Act states that the nominated authority for port security shall be issued by the Swedish Government (SFS 2006:1209). In Ordinance (2006:1213) the responsibility is dedicated to the STA. Obliged by the Ordinance, both the Swedish Police Authority and the Swedish Customs Agency are required to aid and support the STA in the supervision and safeguarding of port security related activities (SFS 2006:1213). In 2007, regulation SJÖFS 2007:1 entered into force. The Regulation stipulates matters such as; *assessments and plans for port security; duties of the PFSO; requirements/information on drills and exercises for port security; inspections from the STA; etc.* (SJÖFS 2007:1).

3.2.4 Summary of the regulatory framework for maritime and port security

In previous sections, a clarification is provided of the fundamental features and structural relationships of the regulatory framework for maritime and port security, existing today at the global, international and national levels. In summary, it is a complex system consisting of different regulations, interests, policies, stakeholders and actors. Therefore, an illustration is provided, in figure 3, to facilitate comprehension of the regulatory system and the influential relationship among them.

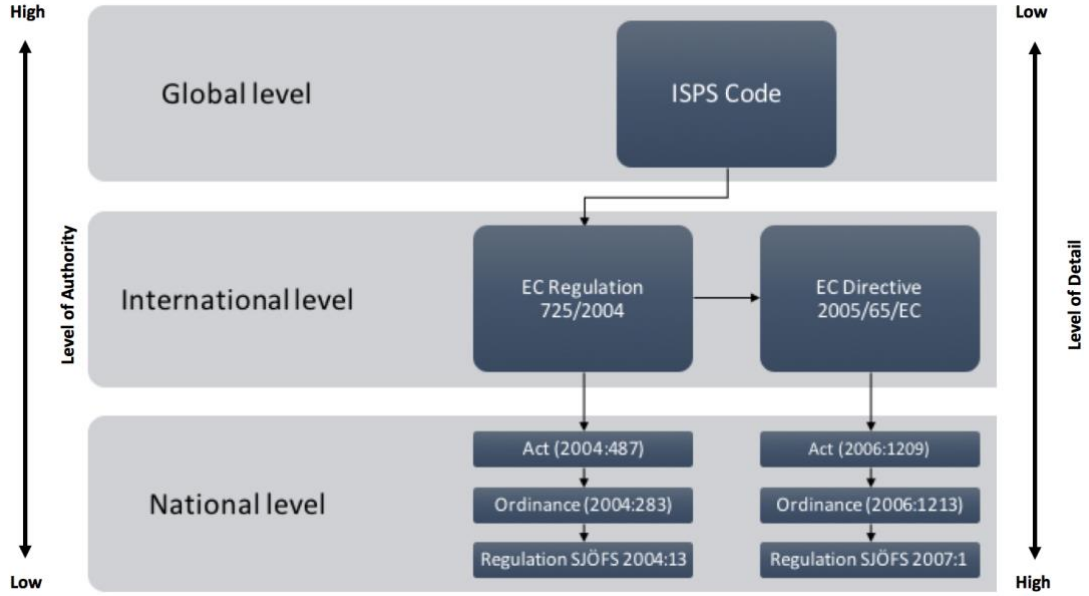

Figure 3: Regulatory framework for maritime and port security (Cole and Winberg, 2018)

The level of authority displayed on the left axis in figure 3 signifies both the geographical area that the regulation covers, from a global, international and national level as well as the level of legal authority. In ascending order, the level of legal authority decreases. All legislations, on the international and the national level, originate from their superiors (illustrated by the arrows). Consequently, this creates a hierarchical legal system of legislations where the ISPS Code is the predominant legal act. The right axis in figure 3 illustrates the level of detail within the legislation. A low level of detail indicates a broader regulatory spectrum while a high level indicates more regulatory detail within the legislation.

3.3 Maritime port security management – a Swedish perspective

The shipping industry represents 90 percent of all globally traded goods (International Chamber of Shipping, 2017). In Sweden, approximately half of all internationally traded goods is directly imported and exported via seaways and 90 percent of all traded goods is at some point during its supply chain on-board a ship (Trafikanalys, 2017). Nonetheless, its significance would have been considerably lower if little or nothing interconnected the land and sea transportation systems together. Hence, ports are regarded as nodes in the current globalised economy (Flynn et al., 2011, Malcolm, 2016). In addition, Andritsos (2013) emphasises, that ports are essential for sustaining the coexistent relationship between different transportation and trading networks.

In the following section, requirements to comply with the regulatory security framework are presented followed by a description of Swedish ports, their owners, size and trade.

3.3.1 Compliance towards regulations – a must to trade

Ports and port facilities are required to comply with the regulatory security framework (International Maritime Organization, 2003). However, the ISPS Code does not specify particular measures that port facilities must take, but instead outlines;

> "*A standardized, consistent framework for evaluating risk, enabling governments to offset changes in threat with changes in vulnerability for ships and port facilities" (International Maritime Organization, 2003).*

With consideration of the above stated, port security should interfere as little as possible with shipping and its "normal" business. Each port and port facility is unique, however, all ports are required to conform to the same international regulations (Mileski et al., 2015). As Wengelin (2006) states, there is a "*comply or die*" condition that ports and port facilities endure as incentives to comply is of the "*whip and not the carrot*". If a port is unable to comply with the required security regulations, the port will inevitably go out of business. Wengelin (2006) continues to argue that no ship would visit a port that is not in submission. The risk of a port stay that ends in a marked record for a vessel and shipping company could have vast complications for future trading as any record that is not clear could have a knock-on effect on affiliated ports and trading partners.

Moreover, as stated by the US Customs and Border protection, during the launch of the Container Security Initiative in 2002, ports should act as the "*last line of defence, not the first*" (Allen, 2006, p. 444). However, the objective of the ISPS Code is to ensure the smooth flow of goods internationally (International Maritime Organization, 2018b). Additionally, a port's security perspective is a dual task as it could be seen as a target in itself, but also as a pipeline for the illegal transport of humans and contraband (Edgerton, 2013). However, it could be argued that when complying with the ISPS Code, a port's primary objective is to ensure that they are not acting as a channel for illegal activities. As Wengelin (2006) argues, IMO Member States are protecting parts of the world from their own foreign policies. He states that the ISPS Code's purpose is commonly interpreted as "*to safeguard ships in my port and this particular port facility"* (Wengelin, 2008, p. 4) and that "*the risk of being the barrel carrying a bullet aimed at an inland target somewhere else in the world is not thought of as the issue at hand*" (Wengelin, 2008, p. 4) even though that is a port's main security function. Germond (2015) and Bueger (2015) further argues that maritime security and the global regulation is about geopolitics where public power by some is projected across a global territory.

Further, Wengelin (2006) claims that rules and regulations do not travel well in space or time. Instead, he challenges that local motives and aims should be constructed in order to achieve meaningfulness to the implementation of security regulations and thus improve compliance towards them. In the same essence, Edgerton (2013) argues that

ports have an exclusive set of challenges they must face and hence entailing that risk has to be assessed at port-, regional- and national level. In contrast, Thai (2009) suggests that a universal checklist to evaluate security management would significantly simplify benchmarking across the globe, and thus lead to an augmented image of the entire maritime industry (Thai, 2009).

On an international (European) level Andritsos (2013) argues that the lack of a unified method for risk assessments in port facilities, both internationally and sometimes even nationally, could negatively affect future improvements of maritime and port security. He states that a standard methodology with available toolkits and instructions together with the establishment of a mechanism for the sharing of sensitive information, where actors may learn from each other on a statistical level could largely improve the implementation of maritime security regulations. Regardless of advocating an improved global methodology, or a more locally adapted security regime, all the published studies seem to agree that improvements are required, even if they propose different methods in approaching a common solution.

Furthermore, incentives to comply with the regulatory security framework can affect the degree of compliance and consequently insurance rates within the sector (Edgerton, 2013). As stated, the ISPS Code is aimed at desired security outcomes, rather than at the method in which they are reached (Edgerton, 2013, Mileski et al., 2015). The economic incentive is important (Edgerton, 2013), and as indicated a port will not be able to continue its business unless it is conforming to the security regulations (Wengelin, 2006). However, a basic compliance is not the same as an elevated security observance. Since the ISPS Code has no incentives built in to its structure, private actors could struggle to be motivated to enhance their rudimentary security level (Edgerton, 2013). This view could be seen as interesting from a private versus public port entity and any distinction they may have in their port security acquiescence. However, introducing an integrated approach to maritime security, where the objective is replaced by the notion of security as an enabler, could allow for maritime port security to become a lesser cost and more of an investment, both on an economic and a personnel level (Edgerton, 2013).

3.3.2 Swedish ports and port facilities

Sweden has 54 public ports which are geographically concentrated in the southern part of the country according to the Swedish Maritime Authority (SJÖFS 2013:4). Moreover, ownership of Swedish commercial ports is largely dominated by the local municipalities (Maritime Forum, 2013) even though a few ports in Sweden are owned by private entities. Further, there are also examples of ports that have a combined ownership amid the industry and the municipality. In addition, a recent development in Sweden is that the ports are owned by the local municipality, nonetheless, the port facilities and terminals are operated by specialist private companies (Maritime Forum, 2013).

Furthermore, both the size and the amount of goods handled by the 54 public ports in Sweden differ significantly among them (Trafikanalys, 2017). The five largest ports in the country stand for approximately half of the total goods handled in the country (Trafikanalys, 2017), which shows that Sweden has a large number of smaller ports.

The resources allocated, and available for allocation, could hence differ depending on the size of the individual port (Bichou, 2004, Mazaheri and Ekwall, 2009). Furthermore, the type of goods handled could also affect the security processes in the specific entity (Bichou, 2004, Andritsos, 2013). The project *Hamnstruktur och Sjöfart* (Sjöfartsverket, 1999) distinguishes between four main categories of submarkets; [1] *ferry and roll-on roll-off (ro-ro) traffic*; [2] *container and lift-on lift-off (lo-lo) traffic*; [3] *specialised transportation;* and lastly; [4] *bulk and general cargo*. When comparing different types of terminal(s) the imminent threat can differ substantially (Bichou, 2004). For instance, a cruise terminal handles great quantities of mostly non-dangerous cargo and is only accessible for a small amount of (trusted) permanent persons. On the contrary, a passenger terminal has lesser amounts of cargo to handle, where almost none are dangerous, but can have a very large number of non-identified persons moving around. Further, a terminal handling oils and chemicals deals with large volumes of dangerous cargo and is again only accessible for a small amount of (trusted) permanent workers (Andritsos, 2013). To assess the threats and risks could hence considerably differ depending on the type of cargo handled at any port.

Moreover, from a Swedish port management perspective there are many actors that are, and are required to be, involved in ensuring maritime port security. Predominantly, the Swedish Transport Agency (STA) is the largest influencer as a single actor for ports position to ensure compliance towards the regulatory security framework (International Maritime Organization, 2003). Further, actors that are acknowledged as being of importance (in Sweden) include the Swedish Coast Guard (SCG), the Swedish Police Authority (SPA) and the Swedish Customs Agency (SCA) (Wengelin, 2006). The STA holds the main responsibility for ensuring compliance towards maritime security regulations (Swedish Riksdag, 2005). The STA is also liable for the coordination of responsibilities among the actors. Whereas the STA has the main responsibility for maritime security, the other organisations have their own areas of accountability (Swedish Riksdag, 2005).

Further, in Sweden , the SPA is principally responsible for setting the security levels in Swedish ports and port facilities after consultation with the STA and the SCG. Thus, the SPA also has the governing responsibility to continuously evaluate the current threat level and summon the other main actors to regular meetings where the prevalent situation is reviewed (Swedish Riksdag, 2005). Additionally, the SCG, SCA and STA are obligated to report any information that may have an impact on the decision for setting the security level. Moreover, the SCG is only responsible for receiving and administrating the reporting obligation of vessels entering Swedish ports and is not involved in port security (Swedish Riksdag, 2005). Likewise, the SCA has a very limited accountability and its only obligation is to report activities or information that could have an impact on maritime and port security to the other actors (Swedish Riksdag, 2005). Figure 4 illustrates the Swedish network for maritime and port security and the individual actor's areas of responsibility.

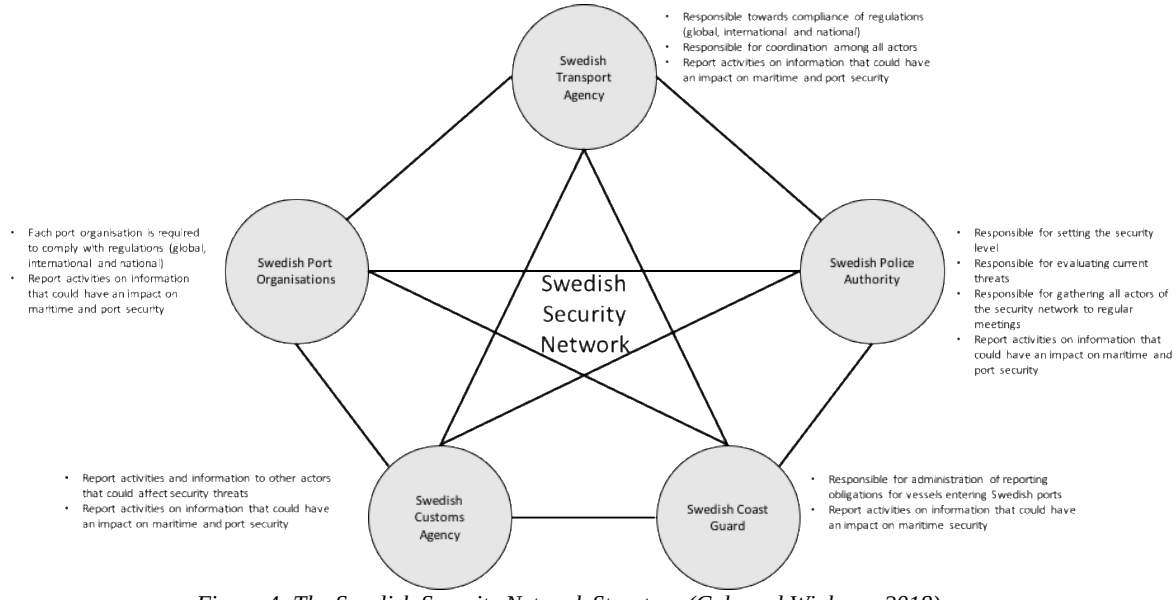

Figure 4: The Swedish Security Network Structure (Cole and Winberg, 2018)

3.4 Principles in port security management

In the section below, an introduction to High Reliability Organisations (HRO), knowledge-creation, organisational learning and security culture that could potentially improve and affect compliance towards the framework of maritime security regulations is presented. Finally, the inter-organisational effort, the security network, to ensure the threat mitigation in Swedish port organisations is presented.

3.4.1 High Reliability Organisations

The potential threats, both human and natural, that ports and port facilities opposed could have disastrous consequences (Bichou, 2004). In environments of such a character, the organisational performance has been duly studied and labelled as HROs. The theory of HROs was developed when researchers studied aircraft carriers in the late 1980's (LaPorte and Consolini, 1991, Roberts et al., 2001). Examples of established HRO's are nuclear power plants, aircraft carriers and emergency and intensive care units. The stated organisations are all operating in high-risk environments with a low number of incidents. However, any potential error or mistake could result in fatal and devastating consequences. Researchers have created a set of criteria to handle risk in such an organisation; *sufficient financial- and human resources*; *high mission valance;* and; *high public awareness* (LaPorte and Consolini, 1991, Roberts et al., 2001).

Today, a port and port facility is not commonly recognised as a HRO (Wengelin, 2012). However, as a consequence of the 9/11 terror attacks, where airport security failed in several areas to operate securely and efficiently, a decision was made to establish airport security organisations as HROs (Wengelin, 2012). In return, more resources was given to airport security and thus creating high mission valance resulting in a new and improved security structure within the airport sector (Wengelin, 2012). Through studying available organisational theories and learn from practical examples, such as the development of airport security, port and maritime security could revise and improve current security regulations. As a result, this could improve the mission valance in order to further mitigate threats and risk within the sector (Wengelin, 2012).

3.4.2 Knowledge-Creation, Organisational Learning and Security Culture

Knowledge-creation and organisational learning are of vital importance to any organisation. If successfully managed and organised it could provide incitements and influence upon the performance and sustainable development of the business (Argote and Miron-Spektor, 2011). Furthermore, Eddy et al. (2006) and Dai (2012) both advocate the significance of organisational learning, as it could contribute to innovation and competitive advantages for the organisation. Knowledge-creation emerges when an individual acquires new knowledge from direct experience of an event (Mitchell and Boyle, 2010, Argote and Miron-Spektor, 2011). In addition, organisational learning is the process of creating, retaining and transferring knowledge within the organisation (Argote and Miron-Spektor, 2011, Berta et al., 2015).

Furthermore, an organisation's capability to understand the value of new knowledge and information, as a part of the learning process and its application, is of significance to elaborate high-quality decisions (Berta et al., 2015). According to Ekow (2011) a organisation, operating in a high-risk environment, must establish a culture built on trust where the persons of the organisation can share their perspectives of risk perception and feel safe to express their opinions. In addition, there is a chance of missing out on important sources of information about risks if an organisation is unwilling or incapable of integrating their personnel into security related activities and processes. Consequently, this could result in negative effects on organisational learning and inhibit the learning processes related to security (Ekow, 2011).

Cultural aspects of an organisation, i.e. organisational culture, could be described as the shared values, beliefs, norms and assumptions of the individuals within an organisation that eventually affect the employee's attitudes, decisions and behaviours (Alvesson, 2002, Martins and Terblanche, 2003, Linnenluecke and Griffiths, 2010, Pietersen, 2017). Organisational culture provides a general framework of unexpressed principles for the organisation and its employees. Furthermore, it influences and shapes the business, both internally and externally. Consequently, it provides a foundation for communication and mutual perceptions on how problems are to be solved and decision-making is executed (Martins and Terblanche, 2003). Security culture could be regarded as a subculture to the organisational culture, that focuses on security. According to Roer (2015) security culture is defined as:

> "*The ideas, customs and social behaviours of a particular people or group that helps them be free from threat and danger." (Roer, 2015, p. 12)*

Moreover, maritime and port regulations and requirements associated with security, should only been contemplated as a first step in the approach to assure and obtain a secure business (Liwång et al., 2015). However, it is the individual company's obligation to ensure that effective and efficient security management is attained, outside the limits stipulated by the regulations (Liwång et al., 2015). Furthermore, Sadovaya and Thai (2016) argue that maritime organisations that lack in knowledge and understanding of how effective security regulations are, tend to become more reluctant to the implementation of the requirements.

In order to achieve a high level of security within the organisation it is essential to establish a security culture, where knowledge-creation and organisational learning are the key elements in developing and increasing the personnel's' perception and awareness of threats (Ekwall and Rolandsson, 2013). A successful culture, unrestrained by strict routines where employees feel safe to express their thoughts, can facilitate learning within the organisation (Argote, 2013). Furthermore, Thai and Grewal (2007), have identified that different security aspects have different impacts on the efficiency of maritime security management. Security awareness (through education and training) was regarded as the most important feature (Thai and Grewal, 2007).

Furthermore, a report submitted by the Australian Government through the IMO, emphasised the need of an adequate security culture and awareness within port organisations (Australian Government, 2018). The report stresses that security culture is something that develops over time through; [1] *"high level commitment from management and staff to achieve maritime security outcomes";* [2] *"appropriately developed and implemented risk-based security measures and procedures";* and; [3] *"targeted and recurrent training high levels of security awareness among staff"* (Australian Government, 2018, p. 3). If not sufficiently managed and organised, a port can become exposed to security risks and threats that could jeopardise the daily operations and the long-term survival of the organisation (Australian Government, 2018).

3.4.3 Security network – collaboration across boundaries

Historically, concerns related to security have been regarded as a concern to be managed by the State. However, developments of the security environment in recent years has resulted in an increased understanding of the importance to involve non-state actors in addressing security issues (Chapsos and Kitchen, 2015). The need for an increased collaboration between state and non-state organisations is due to the complexity and wide range of security related factors that constitute a security environment (Whelan, 2016). These cross-boundary relationships, or security networks, where different security agencies work jointly, can according to Gill (2006) be divided into different levels (local/regional, national and international) and sectors (state, corporate and communitarian). In an attempt to conceptualize an actor network, Whelan (2016) provides the following definition:

> *"…a network can be defined as a set of actors (or 'nodes') that have relationships (or 'ties')." (Whelan, 2016, p. 312)*

Moreover, a security network is an interlinked constitution of different actors, such as governmental, communal, academic, corporations and individual agencies that collaborate and form relationships in order to address and improve security (Dupont, 2004). Collectively, the actors establish a structure of governance, wherein information and knowledge is being interchanged between the actors, with the purpose to achieve common goals (Whelan, 2016). Networks could be considered as an important and necessary instrument in order to tackle complex issues and manage risks effectively (Ebers, 1997, O'Toole, 1997). Nonetheless, the very success and existence of networks is dependent upon the actors involved and their continuous loyalty towards the system and its structure (Whittle and Spicer, 2008).

Furthermore, Brewer (2014) argues that the purpose of the ISPS Code itself is to provide a foundation for integration that unifies various actors in cross-boundary collaborations on different levels (local/regional, national and international) to further enhance maritime security. In recent years, there has been increased attention from, i.a. the EU, towards the importance and strategic value to effectively manage and organise such networks and the structural relationships among the actors within it to further enhance maritime security on an global level (Chapsos and Kitchen, 2015). In the Maritime Security Strategy provided by EU in 2004, the emphasis for increased collaboration and joint responses from all Member States in an effort to provide maritime security, is highlighted. Noteworthy, is that four out of the eleven objectives specified in the strategy relates to increased collaborations and a strengthened maritime security network (Council of the European Union, 2014). As stated in the report, one aim is to:

> *"Promote coordination and the development of further synergies with and amongst Member States, including at regional level, and cooperation with regional and international partners and organisations" (Council of the European Union, 2014, p. 6)*

In addition, Wengelin (2006) has studied the actor network structure of the Swedish maritime security environment. Aligned with the conceptualisation of security networks presented by Gill (2006) and Wengelin (2006), Eski (2016) further contributes to the reasoning that networks could be divided into different sectors (state, corporate and communitarian). For example Wengelin (2006) addresses that the sector relationships tends to be inadequate due to the inability of the different actors to realise their roles and responsibilities in the maritime port security environment. Here, Whelan (2016) recalls the increased tensions due to the conflict of interests and different opinions among the actors, that can influence the performance and effectiveness of the network. Confirmed by Wengelin (2012) in his research, this issue was apparent during the implementation phase of the ISPS Code for all the port facilities in Sweden. Frictions clearly seemed to emerge between port operators and the authorities as a result of separate interests and disparate interpretations of the ISPS Code. Thus, this resulted in the distrusts and rising oppositions among the actors that consequently had a negative impact on collaborations within the security network (Wengelin, 2012).

3.5 Identified theoretical gap

The literature review showed a gap in published research that aims to identify barriers that potentially exist in complying with the regulatory security framework. From a Swedish perspective, studies have been conducted regarding the implementation of the ISPS Code (Wengelin, 2006, Mazaheri and Ekwall, 2009, Hellberg, 2009) and have focused on the financial resources required for the implementation. Thus, a lack of publications on the full compliance of all regulations and their alignments, together with potential barriers, has been identified from a Swedish perspective.

In addition, the review of the literature indicates potential barriers towards compliance have been recognised from previously published research and have been applied to the

propositioned model in this thesis. Thus, it is intended that the selected barriers and their references will be of an integral importance to achieve the studies objectives.

Furthermore, several researchers argue that maritime security studies are a fragmented field of research (Helmick, 2008, Germond, 2015, Eklöf Amirell, 2016). Germond (2015) states that even if the field has interested many scholars, the dimensions of geopolitics is still vastly unexplored and that the topic requires more debate. Moreover, Helmick (2008) positions himself with the principle that the fragmented field could potentially lessen the responsiveness to current and new threats. Additionally, Bueger (2015) asks the question, what is maritime security. By asking this question Bueger (2015) reasons that stakeholders and actors would be allowed to disagree and agree and thus chart what areas in the field require additional studies and interdisciplinary studies for the maritime security studies to be developed. Finally, Eklöf Amirell (2016) upholds that the current maritime security studies of today is a prospering field. However, he claims that it is too closely linked with the needs of stakeholders and is required to be more independent. This would permit the subject matter to challenge old beliefs and harvest new and perhaps unexpected knowledge.

Due to this, the thesis intends to perform a part in unifying maritime security studies by approaching it from a purely academic and non-stakeholder or policymaker position. In addition, it will also aim to contribute to narrowing the gap in published research, by focussing on the barriers towards complying with the regulatory security framework from a Swedish perspective.

3.6 Barriers towards compliance of the regulatory security framework

In table 3 below a presentation of the identified barriers based on published research towards the legal compliance of the regulatory framework for maritime and port security.

Table 3: Barriers towards compliance of the regulatory framework for maritime and port security

Barriers	Description	Reference
Lack of sufficient security network	Conflict of interests within the Security Network influences the performance and effectiveness of the network	Whelan (2016) Wengelin (2012)
	Lack of understanding of responsibilities within the Security Network	Wengelin (2006)
	Inadequate collaboration and relationship between the actors of the Security Network	Wengelin (2012)
Lack of adequate security culture	Inadequate management of security culture and education and training in security awareness can result in increased exposure to security risks and threats	Australian Government (2018) Thai and Grewal (2007)
Lack of resources for implementation	Financial	(Mazaheri and Ekwall, 2009) Edgerton (2013) Hellberg (2009) SafeSeas (2018)
	Knowledge	Sadovaya and Thai (2016)
	Personnel	Edgerton (2013)
Complex and inadequate security regime	Reluctance to implement security measures due to the lack of knowledge and understanding of security regulations and their effectiveness	Sadovaya and Thai (2016)
	Global and international regulations do not conform with national settings and their security environment	Edgerton (2013) Thai (2009)
	Lack of global and international tools, methods and techniques to ease compliance towards regulatory framework	Andritsos and Mosconi (2011) Thai (2009)
	Regulations and guidelines lack in local affiliation to ease compliance and motivation	Wengelin (2006) Edgerton (2013) Germond (2015) Bueger (2015)
	Global versus national interests influence regulations and their effectiveness	Roe (2009) Farrell (2001)
	Defining a port is subject to freedom of interpretation due to ambiguous regulations	Andritsos and Mosconi (2011)

	Unfeasible and inadequate regulations due to urgent development and implementation process and lack of stakeholder involvement	Papa (2013)
	Generic regulations and guidelines that does not take into account the type of goods handled or type of ships services	Bichou (2004) Andritsos and Mosconi (2011)
Security versus efficiency	Increased and stringent security measures could have a negative impact on the efficiency of maritime operations	Thai (2007)
	Organisations tend to maintain port and maritime security measures at the lowest level required, and instead focusses on cost-efficiency	Edgerton (2013)
	Public opinion influences policy-making more than policy-making influences the public opinion. Results in ineffective and inadequate implementation of security-regimes and measures	Page and Shapiro (1983) Metaparti (2010) Edgerton (2013)
Lack of incentives for compliance with security regulations	Little or no incentives, in global regulation, for compliance and implementation	Edgerton (2013)
	Organisations lack in understanding and therefore tend to regard security as a cost rather than an investment	Edgerton (2013)

Table 3 compiles the published research presented in the frame of reference for each identified barrier and acts as an aid in recovering primary data for the deductive research. With the support of the table presented, a questionnaire has been created; the result and analysis is presented in the next chapter.

4 RESULT AND ANALYSIS

In this chapter, the data collected from the survey is compiled and presented in the figures as well as analysed when and where appropriate. Moreover, data collected from the interviews carried out with leading experts in the field of maritime and port security, together with an interview with the Swedish Transport Agency (STA), is also presented. By accumulating the result from the quantitative and qualitative data, the main research evidence of this study was formed by the gathered responses fundamental to the analytical process and the subsequent final outcome. Furthermore, in order to provide distinctness and comprehensibleness to the reader, the chapter has been divided into five sub-parts; Regulatory framework; Security network; Security culture; Barriers towards compliance; and; Summary of main empirical and analytical result.

4.1 Regulatory framework

Based on the findings from the theoretical framework it was concluded that the regulatory framework for maritime and port security in Sweden consists of nine different legislations. Furthermore, the maritime and port security legislation is comprised of five levels of authority, where superior regulations are in the descending order from global, to international and the national judicial system. In order to fulfil the requirements, Swedish ports have to comply with all nine legislations.

In the following part, the results from the survey and interviews, that were analysed, are presented. The presentation of the findings, focus on the perceived ability of Swedish ports to comply with the regulatory framework for maritime and port security. In the search of possible constraints or tendencies, that might limit the ports perceived capability to fulfil the requirements, the survey result was analysed based on varying data classifications.

4.1.1 Compliance towards regulations

To comprehend whether or not a compliance issue was prominent, the participating ports were asked in the survey to grade their perceived degree of compliance with the individual legislations. The surveyed ports were asked to grade their perceived compliance from one to five, where one was equal to the lowest degree of perceived compliance and five was equal to the highest degree of perceived compliance.

In figure 5, the results from all the respondents of the survey, for each category (by regulation), are presented. The outcome indicates that there is a wide-range of perceived compliance among the respondents. Since the result presented provides an indistinguishable understanding of the actual constraints, the data was further analysed.

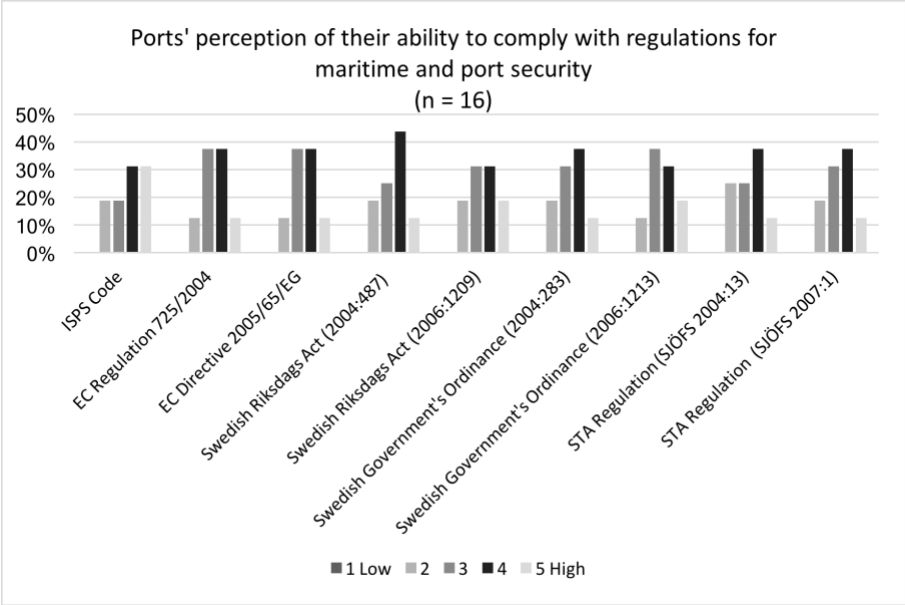

Figure 5: Perceived compliance with regulatory security framework

The following figures (figure 6 and figure 7), the same data was applied as in figure 5, with the exception of one respondent who chose to be anonymous, and thus could not be categorised. However, an average score of each individual respondent's perceived compliance towards all legislations was carried out and summarised. In figure 6, the data were categorised into the regulations at the global, international and national levels. Moreover, as an extension and comprehension to the perceived compliance at different levels of authority (presented in figure 6) the national level was further divided into the categories of Swedish Acts, Ordinances and Regulations (see figure 7).

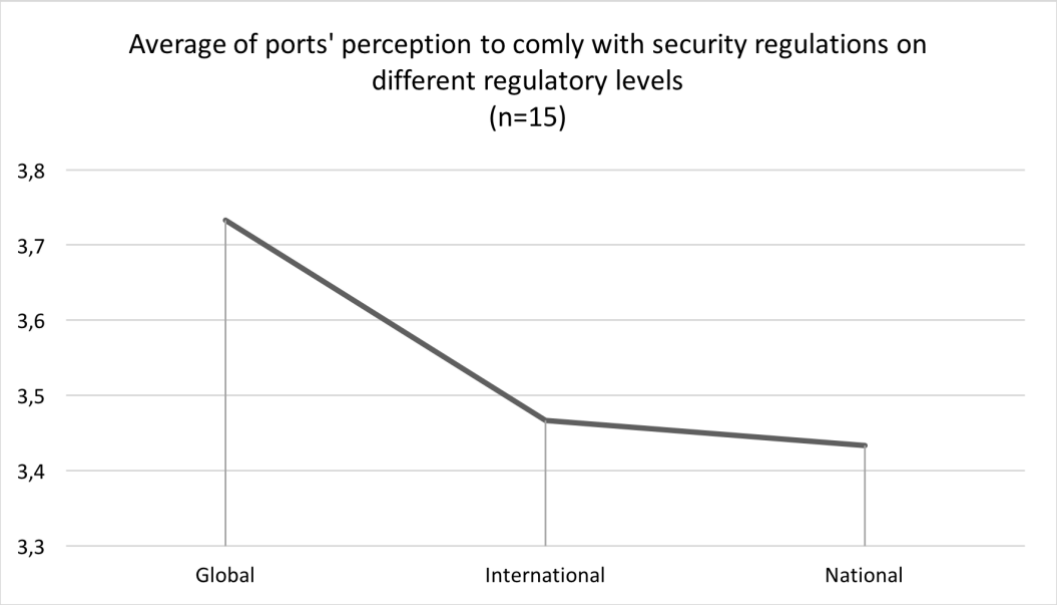

Figure 6:Average perceived compliance with security regulation

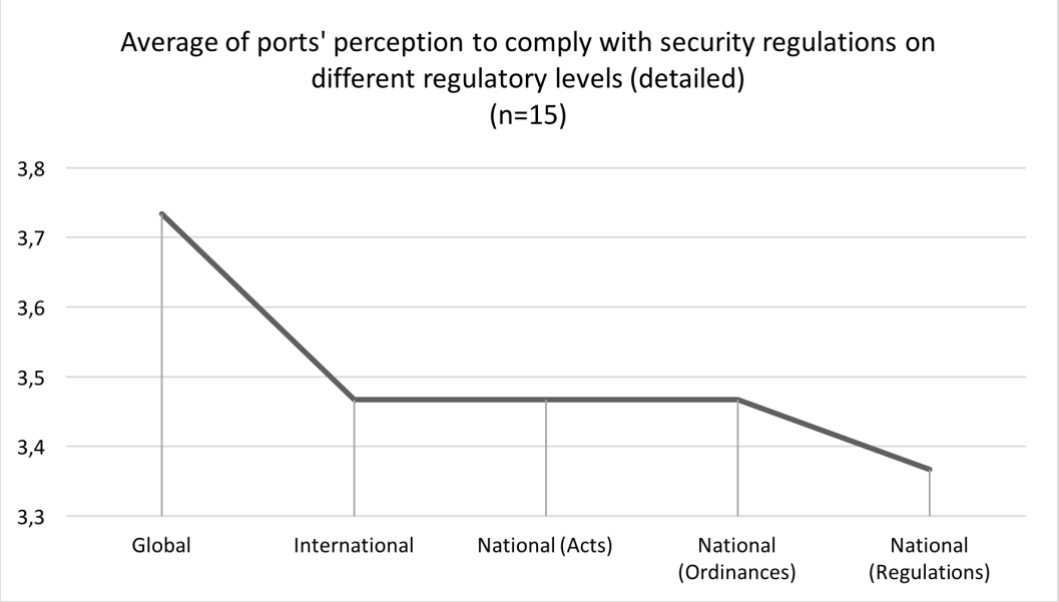

Figure 7: Average perceived compliance with security regulation (detailed)

In both figure 6 and figure 7, there is an apparent trend signifying that the degree of compliance towards the global regulation differs in comparison with both international and national regulations. In this respect, Swedish ports perceive it to be more difficult to conform with the national legislations for maritime and port security, than the regulations on superior levels. According to the distributed survey, the Swedish Transport Agency (STA) regulations for maritime and port security were identified to pose the greatest challenge to comply with, as presented in figure 7.

According to one interviewed respondent, the main reason that Swedish ports experience it to be a greater challenge to comply with the national regulations than with global and international regulations, can be due to the competitive market situation. Furthermore, the respondent provides an explanation to why Swedish ports experience it to be less difficult to comply with the regulation on a global level by stating that:

> *"... the ISPS Code is so embedded into the security plans, instructions and routines that one does not question it. However, everything else that a port should comply with, that is not as embedded." – LE*

In comparison, another respondent stated that:

> *"A global regulation, like the ISPS code, will be experienced as more blunt for some, than for others." - SA2*

Regardless, if global regulations are blunt or not, they must be complied with, otherwise a port will lose business. Hence, the same respondent continued the reasoning by contending that:

> *"Regulations are deal qualifiers. You cannot attract new customers if you do not comply with the regulations. However, complying ensures you keep the customers you have. From a business perspective, all you have to do is comply with the regulations and then other things will attract business." - SA2*

On an international level, the European Commission's (EC) Regulation and Directive may be regarded as unnecessary by the ports. Particularly, one respondent considered it to be a protruding issue when ports are in possession of a deeper knowledge regarding the security regulations. The EC Regulation and Directive require the ports to go further in their security work, which implies that they are not necessarily competitively neutral on a global level. Moreover, the security regulations on a global and international level receive more attention from the ports, this may result in an unintentional gap of insufficient knowledge or understanding in regards to the security regulations for maritime and port security on a national level.

Furthermore, in figure 8, the data from the figure 5 was applied (except from the previously stated anonymous respondent). In order to identify if there were any perceived differences in the degree of compliance depending on the type of ports studied, the responding ports were divided into two categories; ports handling passengers (pax) and ports not handling passengers. An average of the score from the

respondents, in the two categories, was then applied to each individual regulation. The result is presented in figure 8.

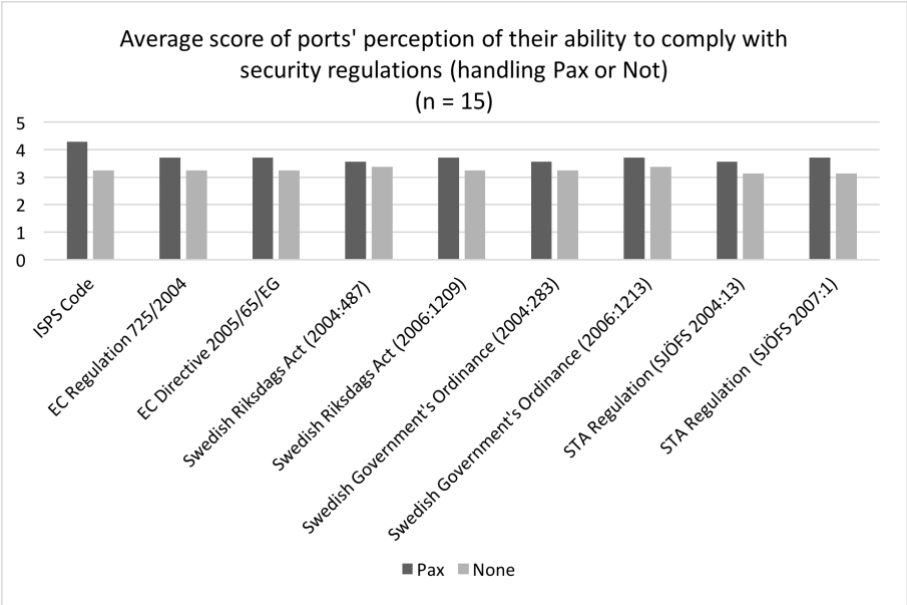

Figure 8: Perceived ability to comply with regulatory security framework

The result presented in figure 8, indicates that there is a perceived difference between ports that handle passengers and ports that do not handle passengers. In total, ports that handle passengers score a higher degree of perceived compliance with regards to all nine legislations, than ports that do not handle passengers. According to one of the interviewees, the reason could be that passengers require another form of risk assessment comparing with other types of goods.

> *"... one recognises a threat when it comes to passengers. If there are many people moving around one is forced to think of what could occur if for example a bomb would go off." - LE*

Moreover, the respondent continued to argue that it can also be the case that passenger ports perceive security as a marketing instrument in order to secure business, which ports that do not handle passengers may not.

> *"... as a port, one wants to sell one's services and as a passenger one wants to see that there is protection, so [security] is some type of market competitiveness." – LE*

4.1.2 Compliance issues and influencers

As mentioned above, ports operate within different environments. Hence, the prerequisites necessary towards compliance with the regulatory frameworks for maritime and port security may differ among individual ports. Published research that was studied in the frame of reference reveal that a lack of resources could affect the implementation and compliance towards maritime and port regulations. Four areas of resources were recognised; [1] *Personnel*; [2] *Time*; [3] *Financial*; and; [4] *Knowledge*.

Further, the frame of reference recognised that published research had identified areas of improvement required for maritime and port security. The research studied here was divided into two directions of development; more locally adapted regulations and more global tools and methods made available for implementation. Lastly, the reviewed published research stated that the generic maritime and port regulations do not allow for types of goods and vessels handled in the various ports to be considered in the security work. Based on the above statement, data was collected and analysed; the results are presented below.

4.1.2.1 Resource availability

In figure 9, the perceived available resources, applied towards compliance with maritime and port security regulations, from the surveyed ports are presented. As stated, the resources are divided into four groups; [1] *Personnel*; [2] *Time*; [3] *Financial*; and; [4] *Knowledge*. The surveyed ports were asked to grade their perceived availability of each individual resource from one to five, where one was equal to the lowest degree of perceived resource availability and five was equal to the highest degree of perceived resource availability. Figure 9 is presented in percentages, where the result from all the surveyed Swedish ports are listed. Categorised by the different resources, identified in the theory as critical components towards compliance, it shows a widespread result of perceived values.

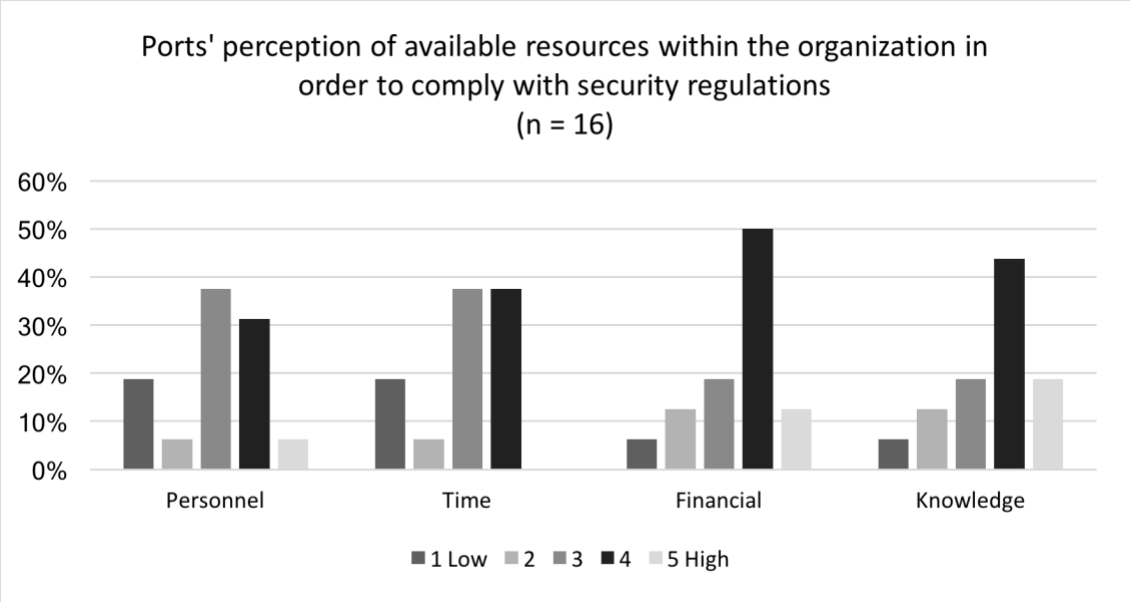

Figure 9: Perceived resource availability

Presented in figure 10, the same data collected was used as in figure 9, except from one respondent who chose to be anonymous in the survey and thus could not be further categorised. A perceived average of all the respondents' score, based on the individual resources, was analysed. This was done in order to facilitate the understanding of which resources Swedish ports considered to be the most available to them and what they perceived to be lacking in order to fulfil the requirements in the regulatory framework for maritime and port security. The result shows that time and personnel availability were considered the most absent resources. Meanwhile, both financial and knowledge resources were considered to be of a higher accessibility for the organisations.

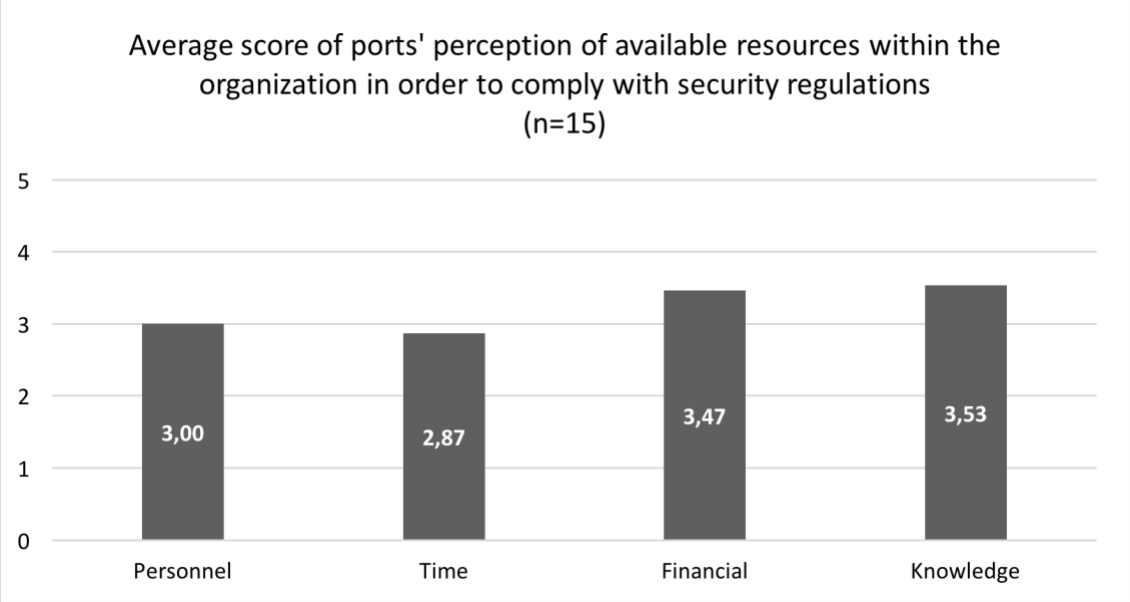

Figure 10: Average perceived resource availability

However, even if resources are claimed in the frame of references to be of importance to compliance, one interviewee stated that more resources made available to the ports does not necessarily result in a better compliance towards security regulations.

> *"... more resources do not necessarily solve the issue of compliance. If you have more resources, you will do more of what you experience to give the best reward and that is not necessarily complying to a regulation."* - *SA2*

Nevertheless, another respondent stated that all resources given to the ports are of importance in order to achieve a greater security compliance. To simply increase the security budget, but not evaluate the other available resources, will not yield the desired outcome of better compliance.

> *"I believe it is a combination of resources. One cannot just have a lot of money, but there has to be a combination of good employees and knowledge."* - *LE*

Moreover, the responding ports were divided into two categories; ports handling passengers and ports not handling passengers. The result indicated that on average, ports handling passengers have a higher degree of perceived value of resource availability within their organisation. This is applicable to all the resource categories and is illustrated in figure 11.

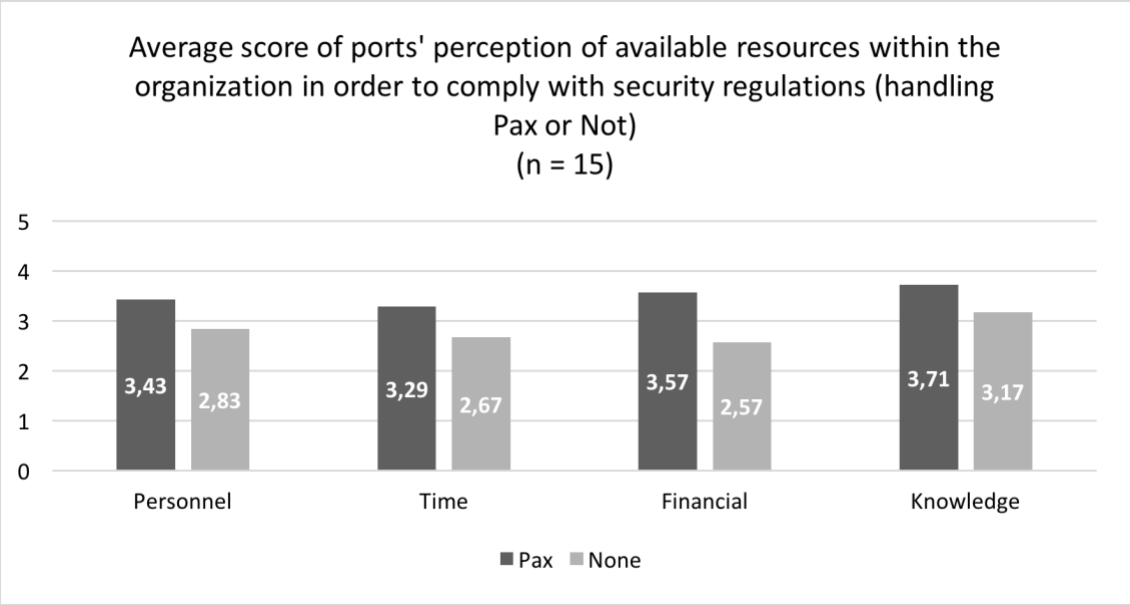

Figure 11: Average perceived resource availability (pax or no pax)

A reason for passenger ports perceiving to have more available resources could be that passenger ports prioritise differently than ports that do not handle passengers. If security is not functioning well in a passenger port the attention from the public will most likely be greater than in a port that does not handle passengers. Furthermore, passenger ports have the possibility to transfer the cost involved with security to the customers differently than within goods handling. As stated by one of the respondents:

> *"... it would be a lot more evident if passenger ports do not comply, because they would receive a totally different media attention, which means they prioritise differently. One can also transfer the consumer willingness to pay [for security] differently in a passenger port."* - *SA2*

4.1.2.2 Regulatory compliance in relation to resource availability

In order to identify whether or not there is a correlation between perceived resource availability and a perceived ability to comply with the different regulations among Swedish ports, the two factors were set in relationship with each other. In figure 12 the analysed perceived average of the individual responses, for both the resource availability and the compliance towards regulations, is presented.

Figure 12 provides information considering the average score per port with regards to perceived compliance with all maritime and port regulations (see figure 5) set in relation to perceived resource availability to comply with the regulations (see figure 9). Thus, in order to attain the data used to compile figure 12, a total of thirteen questions were posed to each individual port.

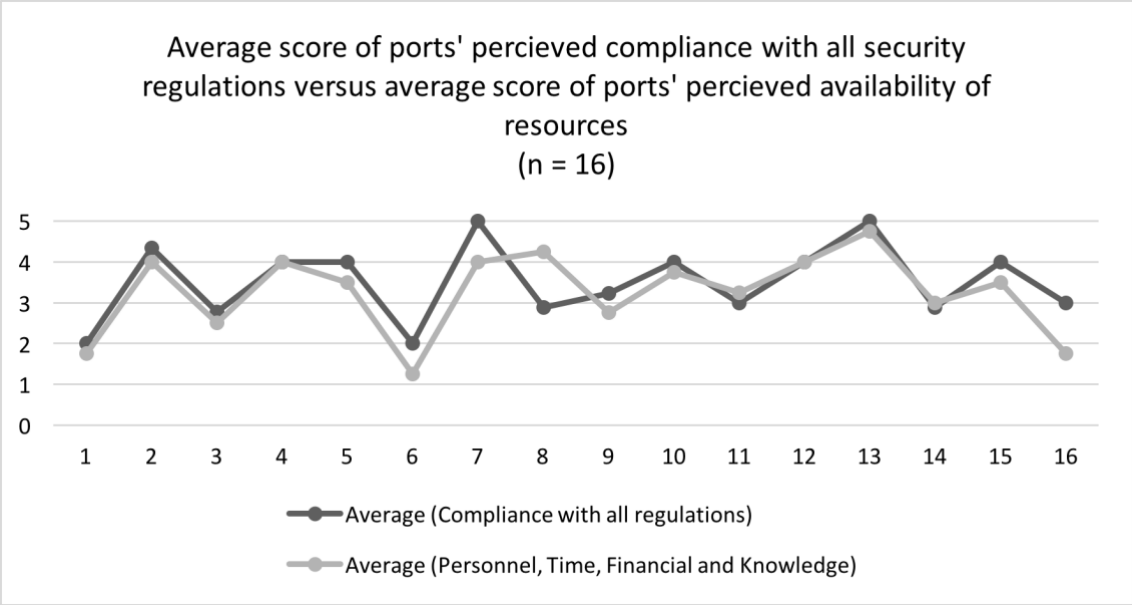

Figure 12: Average perceived compliance versus resource availability

In figure 12, the average of each individual port's compliance towards all maritime and port regulations indicates to have a statistical relationship to that of each individual port's perceived average availability of resources. However, the analysed result shows that some outliners exist. The maximum difference between one individual port's averages is 1,5 on the one-to-five scale.

Furthermore, in response to figure 12, the interviewees did not find the connection between the perceived compliance and perceived resources as surprising. If a lack of resources is evident in a port, the port will focus on what is viewed as the most urgent matter at the given time. Compliance towards regulations may not be top priority on a daily basis, hence, if a lack of resources is evident, compliance may suffer.

> *"The connection that is described [in figure 12] feels very expected. If you have a lack of resources you will target the quicker fixes and that does not necessarily mean compliance towards regulations, but instead ensuring that the traffic is flowing, the commercial parts are prioritised. […] If you ask the ports I am convinced that they claim that they do not gamble, they will simply claim that they are dealing with the most important issues first." - SA2*

Furthermore, another respondent stated that ports may perceive themselves to be better at security than they are in reality.

> *"If a port does not have any incidents or abnormalities to report they will probably consider their security to function well, until something occurs." - LE*

However, when the ports themselves are asked to rank their capabilities the correlation may be more evident than if a study was conducted investigating the ports submitted reports on incidents and accidents compared to the actual available resources.

"... when the ports themselves do the evaluation, one can end up closer in compliance and available resources." - *LE*

4.1.3 Amendments to the regulatory framework

Identified in the theoretical framework, researchers argued that there is a need for the development of the regulatory framework for maritime and port security. However, this was not a shared view among the different proponents of researchers of the process forward for development, and the actions required for further progress. Regardless of the accurate approach contended by the different scholars, this study set out to comprehend the perspective from the ports themselves.

Therefore, to understand the standpoint of Swedish ports, the survey asked the respondents to answer closed-ended questions with "yes" and "no" responses. In the figures presented below, the results from fifteen of the sixteen ports answers are provided. The one port that is excluded, chose to be anonymous and thus cannot be categorised in the studied groupings.

Figure 13 shows data regarding the Swedish ports' belief that the current regulatory frameworks for maritime and port security should be developed. The question purposely did not state or indicate in what direction or way that the legal frameworks should be developed.

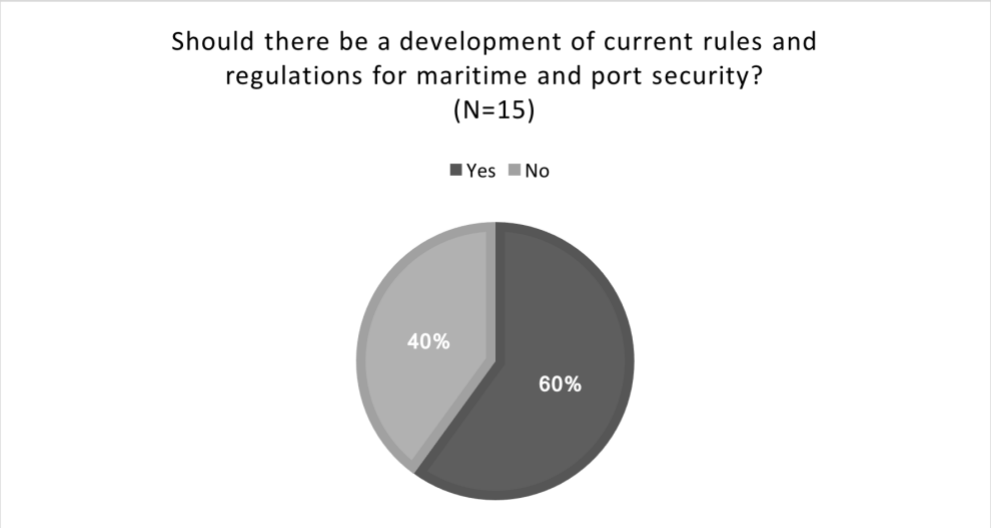

Figure 13: Development of regulatory security framework

As presented in figure 13, a majority of the Swedish ports express a need for a development of the current regulatory framework for maritime and port security.

However, on a global level, there is little belief that the current regulations will be amended. The ISPS Code is considered to be too embedded into the current global trading market and amongst its actors. That, in combination with the fact that security is not currently a significant issue, compared to matters related to the environment which are being prioritised. As stated by one respondent:

> *"Right from the beginning, when the security regulations were created, there was an awareness that things were proceeding to rapidly. However, the detail and contemplation was sacrificed in order to get something up and running […] Instead, a choice has been made to focus on other issues, such as the environment, since there is always something that is more urgent to work with." - SA1*

As further stated by another respondent:

> *"I do not believe that the ISPS Code will be revised. The ports have already implemented it fully and they will not want to change it. This [question] turns into major politics immediately."* - SA2

One respondent moreover states that the security regulations are not an issue and thus will not be revised:

> *"… revising the ISPS Code does not exist on our agenda. I have not heard any discussions or read any reports that raise the question. At the time being, it is simply not an issue." – SA3*

The Swedish Transport Agency (STA) does not believe that the EC Regulation and Directive will be amended in the near future:

> *"[…] There is a quite weak interest in regards to additional regulations within the field of maritime security amongst the European member States. The [EC] Regulation and Directive are written in such a way that new threats can be handled within the existing framework by applying a revised risk assessment and plan. This does not require to amend the current [EC] Regulation and Directive." - STA*

Furthermore, recognised as one of two development directions from the theoretical framework, was that the regulatory framework could be more locally adapted. The survey hence asked the respondents a closed-ended question, with a "yes" or "no" option if they sought-after for maritime and port security regulations to be more locally adapted. In figure 14 and figure 15, the analysed result is presented.

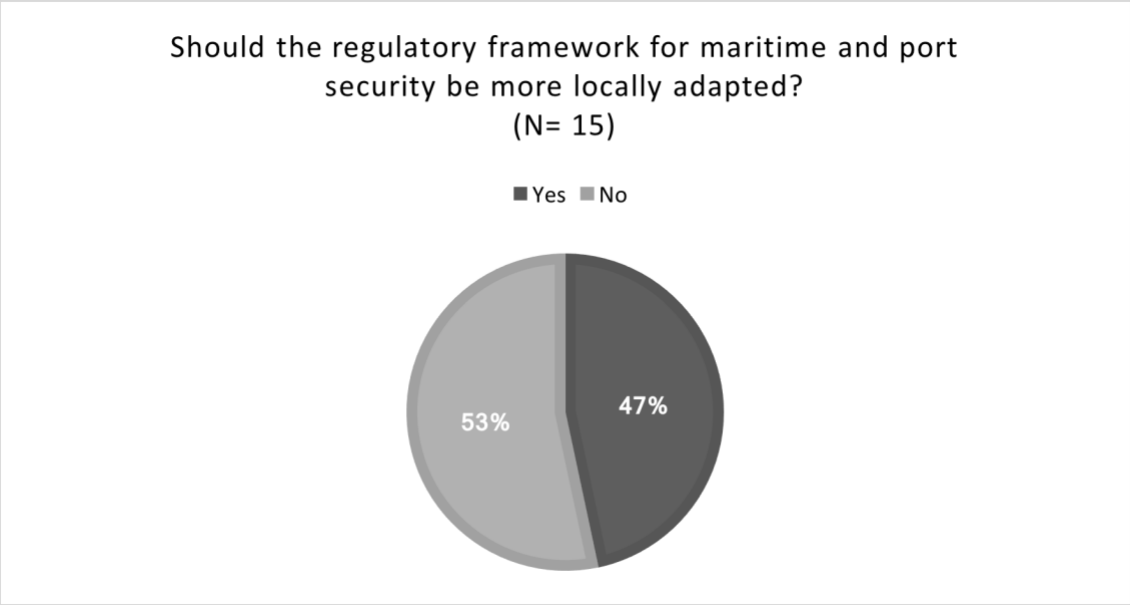

Figure 14: Local adaptions of regulatory security framework

In figure 14, the result indicates that a slight majority of the respondents do not wish for the current maritime and port regulations to be more locally adapted. However, to identify whether there were any correlations in the presented result (figure 14), the collected data was categorised, based on the size of the surveyed ports. Presented in figure 15, the analysed result indicates that smaller ports, to a much greater extent, advocate a need for more locally adapted security regulations. Additionally, the result indicates that larger ports do not wish for the maritime and port regulations to be more locally adapted. Finally, the analysed result of the medium-sized ports indicates a divided point of view.

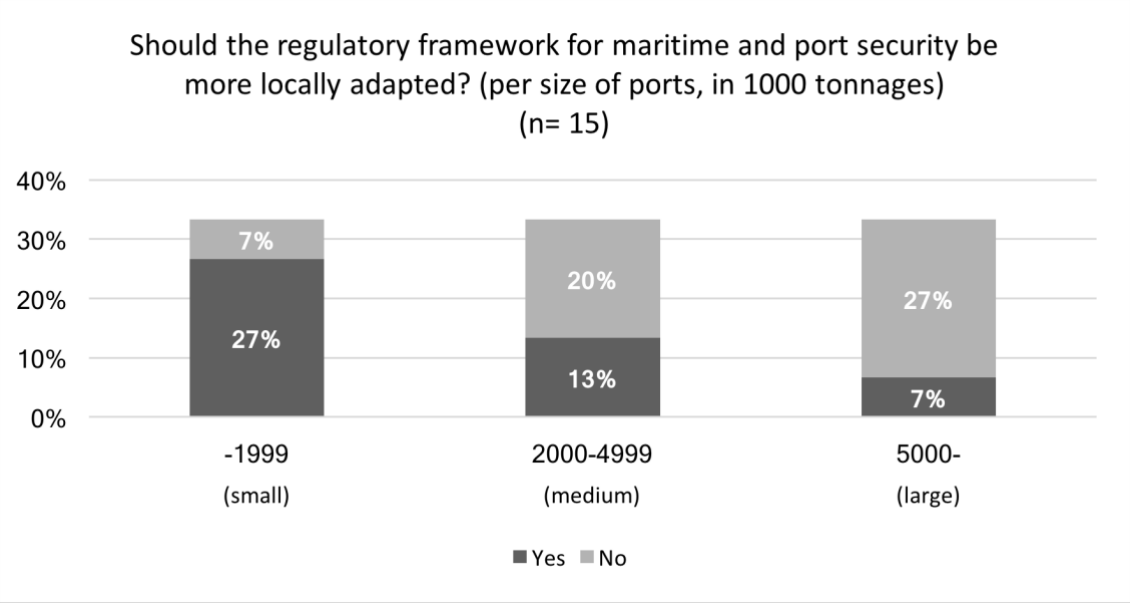

Figure 15: Local adaptions of regulatory security framework (per size of port)

Moreover, the interviewees agreed that there are not any great advantages in locally adapting the current regulatory framework. When individual ports conduct a risk

assessment, that is part of adapting the framework to fit one's local settings. Nonetheless, the individual risk assessments in a port can never conclude that the required security level is lower than that of the minimum required level stated in the regulatory framework. If that were to be acceptable, the entire system would collapse, since the regulatory framework was established in order to keep the supply chain intact, and not allow for any weak spots. As stated by two respondents:

> *"Since shipping is one of the few proper global industries, there is a clear policy advantage with having the same regulations everywhere and thus set-ups such as the ISPS Code through SOLAS are truly good." - SA2*

> *"The State has conducted a risk analysis and it demands that all ports are at least at security level one. […] if a port is reluctant to comply with the regulations, threats can arise at the port that they had not accounted for. This, due to the fact that other ports have protected themselves too well in comparison." - LE*

Additionally, the second of the two directions for development of the current security regulations in previously published studies advocate the need for developing more explicit tools and methods for implementing global and international legislations. Therefore, the surveyed ports were asked if they desired more explicit tools and methods for the implementation of the global and international regulations. This was done by a closed-ended question with the option of a "yes" or "no" answer. The result can be viewed in figure 16.

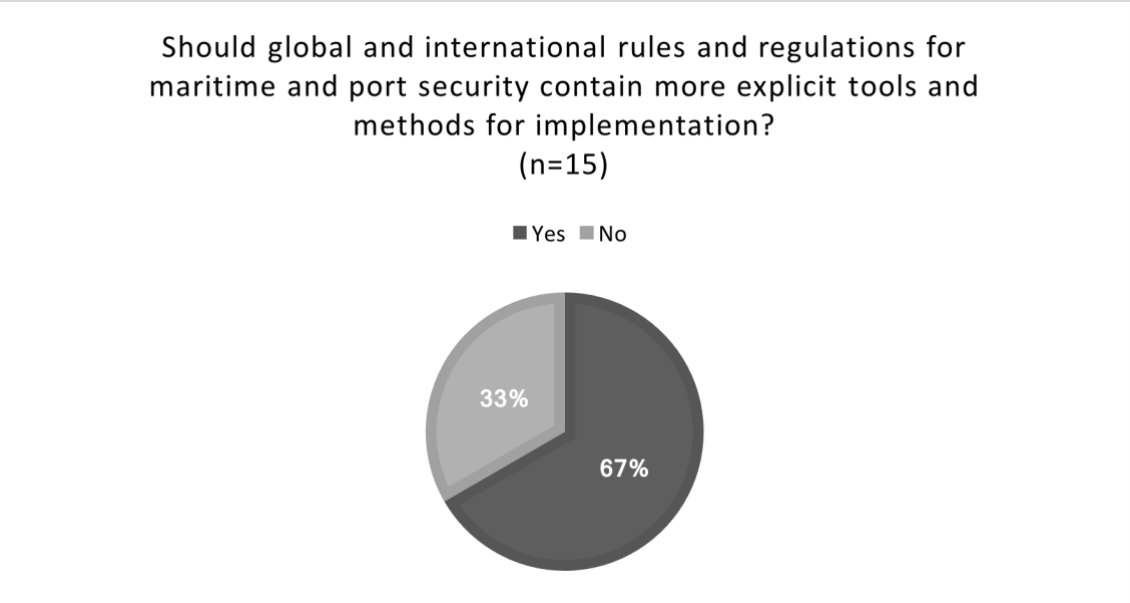

Figure 16: Demand for more explicit tools and methods in regulatory security framework

The result presented in figure 16 implies that two thirds of the surveyed ports desire more explicit tools and methods for implementing maritime and port regulations. One third of the surveyed ports expressed that they do not desire clearer tools and methods for implementation.

To assist ports in their implementation is deemed as a necessity, since ports lack in resources and knowledge. Thus, the authorities should assist the ports by clarifying what they are expected to achieve. As stated by two respondents:

> *"There is a shortage of knowledge, shortage of resources and lack of understanding the complexity of the security problem, so the more assistance the ports can receive, the better." - SA1*

> *"Authorities should make it easier and clearer for the business actors." - SA2*

Additionally, since it was considered as a necessity from a majority of the surveyed ports to develop tools and methods for implementing a global and international regulations, further analysis of the result was considered as essential. Hence, the ports were categorised according to size; *small; medium;* and; *large*. The result can be viewed in figure 17.

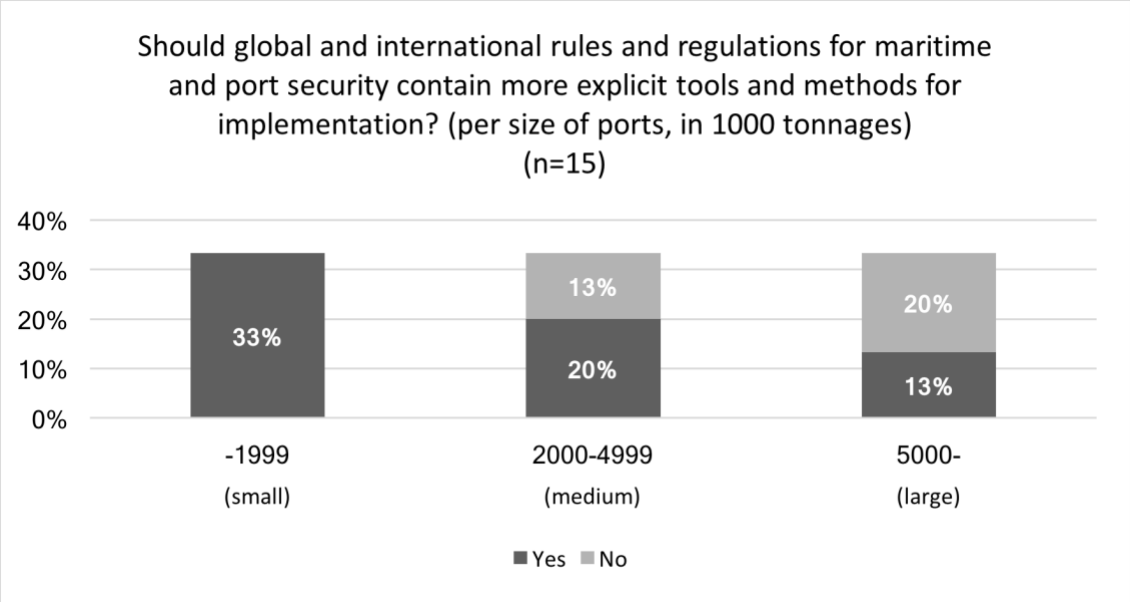

Figure 17: Demand for more explicit tools and methods in regulatory security framework (per size of port)

Seemingly, when categorising the responses based on the size of the individual ports, the result indicated that all the small ports consented to the reasoning for the necessity of having more explicit tools and methods to facilitate implementation. Moreover, a majority of the mid-sized ports agreed with this contention. As presented in figure 17, a majority of the ports categorised as large, did not regard there to be a need for clearer rules and regulations.

The reasoning behind the unified desire from small ports to have clearer tools and methods for implementation could be in correlation with their available resources. A larger port, even if they themselves do not possess the right resources for implementation, have the possibility to acquire the resources required. As stated by one respondent:

> *"Small ports that lack in resources want to know what is required of them. […] The larger the port, the more resources are available to work with security. A major port that does not have their own resources, have the possibility to recruit private security actors, which today have become a meaningful resource."* - *SA1*

Furthermore, as stated by one respondent, smaller ports may not perceive the threat as present as a larger port. Hence, they wish to do what is required from them to be approved by the inspectors, not necessarily because it will enhance their security.

> *"The smaller the port, the lesser one sees the threat as real and the lesser one is willing to do in order to become an 'approved' port. A small port believes it is better to receive a list with items to achieve to be 'approved', so that they do not have to 'waste' resources."* - *SA1*

4.1.4 Adaption of security subject to type of vessel and goods

Moreover, in the survey of the ports, they were asked to grade how much they perceived to adapt their security work depending on the type of vessels and goods they handled. The same scale as previously used, with a scale from one-to-five, was applied. The responding ports were divided into two categories, passenger handling ports and non-passenger handling ports. The average score of the participating ports in their respective category was calculated and the result is presented in figure 18.

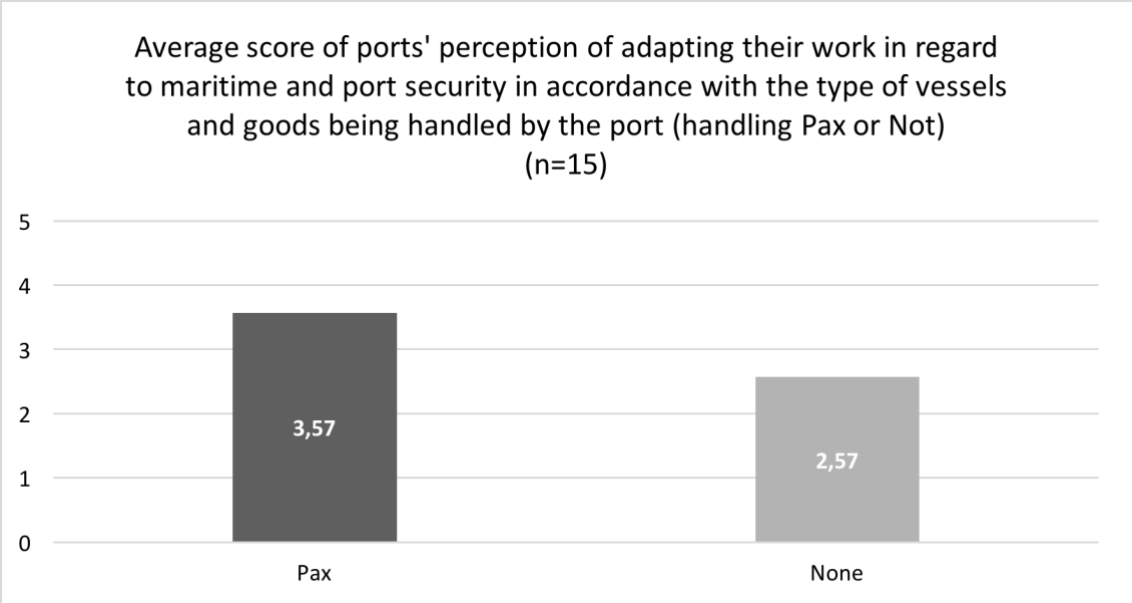

Figure 18: Adaptions (type of vessel and goods) of regulatory security framework (pax or no pax)

Figure 18 reveals that ports that handle passengers have a higher perceived tendency to adapt their security work in accordance with the type of vessels and goods handled, than ports that do not handle passengers. The responding ports were also divided into three further categories, namely; [1] *container and lo-lo (lift-on/lift-off)*; [2] *specialised cargo (such as forest cargo, refrigerated cargo, new cars)*; and; [3] *bulk and general cargo (such as oil, chemicals, gas, coal, ore, grain)*. However, no disparities or patterns were

distinguished among the remaining categories of ports in their perceived adaption of security work in regards to the type of vessel and the goods they service.

Further, the ports were questioned if they wished for the regulations to be more adapted towards the type of vessel and the goods handled. The question was posed as closed-ended with a "yes" or "no" as the possible answer. Figure 19 presents the result.

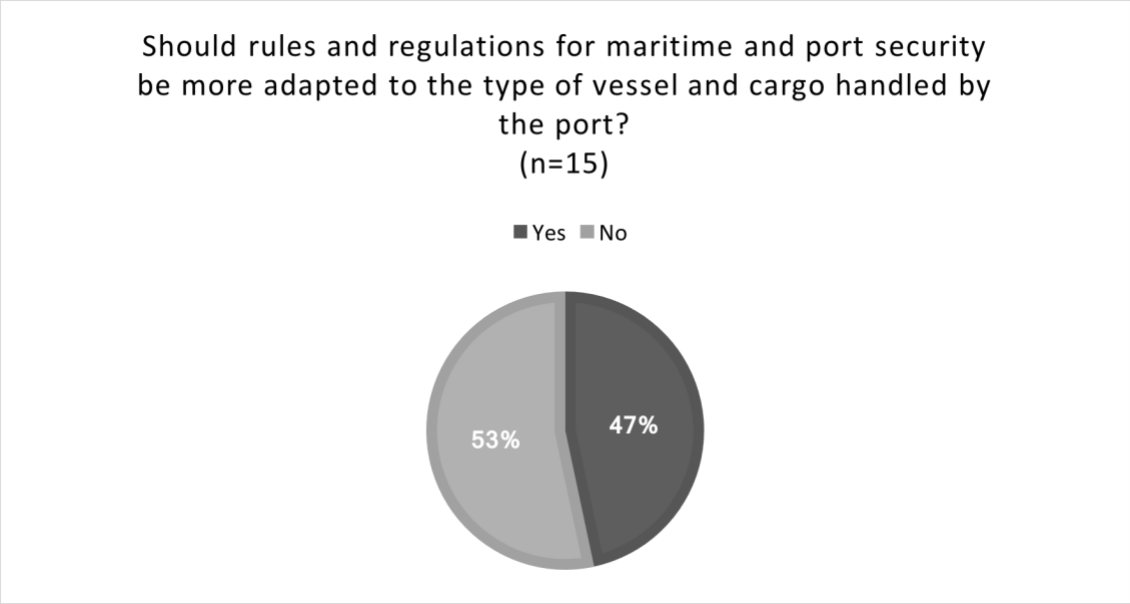

Figure 19: Adaptions (type of vessel and goods) of regulatory security framework

The result presented in figure 19 indicates that a slight majority of the surveyed ports do not wish for the regulations to be more adapted to the type of vessel and the goods handled. Moreover, the same data used for figure 19 was applied in figure 20. However, here the ports were divided into three categories in relation to size; *small*; *medium;* and; *large*; based on the number of tonnes of goods handled annually. The result is displayed in figure 20.

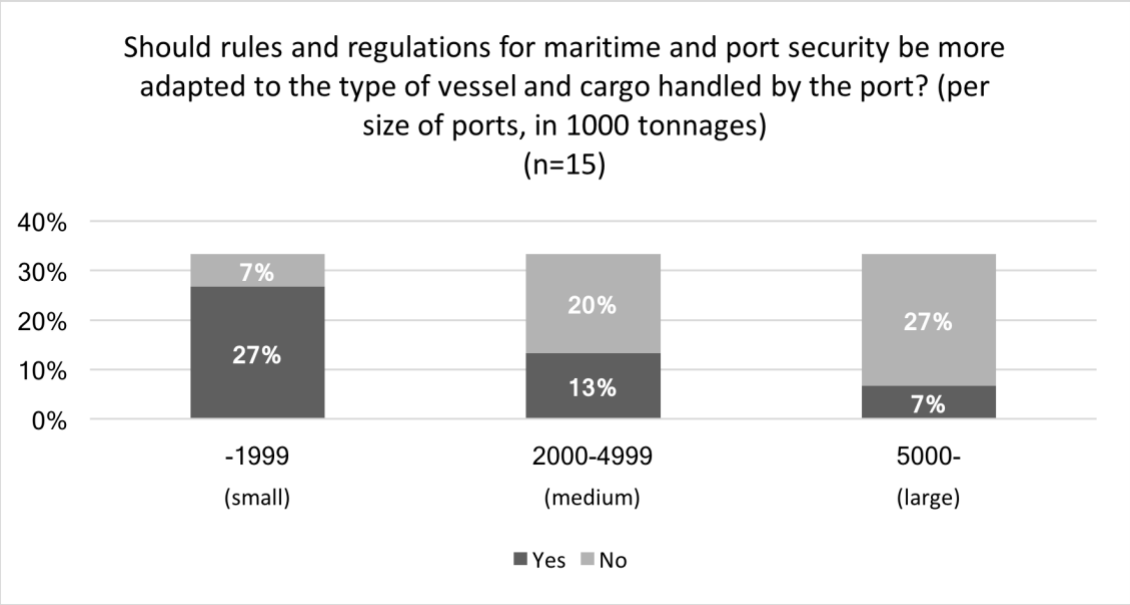

Figure 20: Adaptions (type of vessel and goods) of regulatory security framework (per size of port)

Seemingly, in figure 20, a large majority of the small ports desired for the regulations to be adapted towards the type of vessels and cargo handled in the port. A majority of the medium-sized ports did not consider there to be a need for adapting the regulatory framework in accordance with the type of vessels or goods handled by the port. Moreover, a vast majority of the large ports did not see any requirement for the regulations to be more adapted to the ports' trade.

However, an argument can be stated that the current regulations already allow for adaptation in accordance to the trade of the individual port. Since the ports are required to carry out a risk assessment, they may increase security in certain areas if the assessment deems it to be necessary. Nevertheless, they are not permitted to lower their security level below the standards set by the regulations. As stated by one respondent:

> *"A risk assessment should be conducted and with that one can conclude that certain calls of vessels, at certain times of day, are under a larger threat. […] already today the purpose is that security should be adapted, but […] the ports have to comply with the minimum levels that have been set."* - *LE*

Furthermore, this relates back to the issues raised under figure 14 and figure 15, where the ports were asked if they wished for the regulations to be more locally adapted. The current regulations allow for certain variations within set boundaries. As stated above, the ports should use this to their advantage. However, to be able to carry out such a risk assessment and benefit from it, requires a certain amount of knowledge and confidence; something that smaller ports may lack. As pointed out by one interviewee:

> *"… smaller ports do not have the confidence to carry out a good risk assessment and point out to the inspectors how they perceive the threat level and how they wish to shape their security plan."* - *LE*

The result reveals that smaller ports struggle to see the wider purpose of the current regulations; here they have an argument when stating that they do not have a large threat towards their port. However, for the regulations to function, the entire supply chain must be intact, something that may not be comprehended by the smaller ports.

> *"The smaller ports do have a point in stating that they do not have a large threat level against them. However, the understanding that they could act as a gateway into to the global transportation of goods, there they fail." - SA1*

Further, an issue raised during the conducted interviews was the question of cost and motivation. To implement security measures does not differ tremendously between a small-sized port and a large port. Once they are installed they are installed. However, the incomes generated at a small port are generally lower than at a larger port. Therefore, the cost involved with security is a larger percentage of the total turnover for a smaller port than a larger port. Hence, the task of motivating smaller ports to achieve the security requirements will always likely to be a challenge. As stated by two respondents:

> *"Costs for implementing the regulations do not differ that much from a small sized port and a large port. Once a fence is up, it is up. However, the procedures differ quite substantially between a small sized port and a large port. As a result, a small port will perceive the costs for security as much higher." - SA2*

> *"The EU Directive is not always optimal in all ports. In larger ports it might work very well, however, in smaller ports it can be very hard to motivate the port to accept those additional assessments and plans." - STA*

4.2 The Swedish port security network

As identified in the theoretical framework, a barrier towards the compliance of maritime and port security is the lack of a sufficient and well-functioning port security network. Here, published research has recognised three main items impacting the security network. Firstly, there are conflicts of interest within the security network which influences the performance and effectiveness of the network. Secondly, there is a lack of understanding regarding each of the security actors' responsibilities within the network. Thirdly, there is an inadequate collaboration and relationship between the actors of the security network. Thus, in this part, the results from the survey and interviews related to the port security network are presented.

To comprehend how Swedish ports reflect upon the collaboration with the actors within the Swedish port security network, they were asked to grade their perceived collaboration with the five identified actors of the Swedish security network on a scale from one-to-five, where one is equal to a low degree of perceived collaboration and five represents a high degree of perceived collaboration. In figure 21, the responses from all ports are presented. Categorised per actor/authority, the score in percentage represents all the respondents' answers per category.

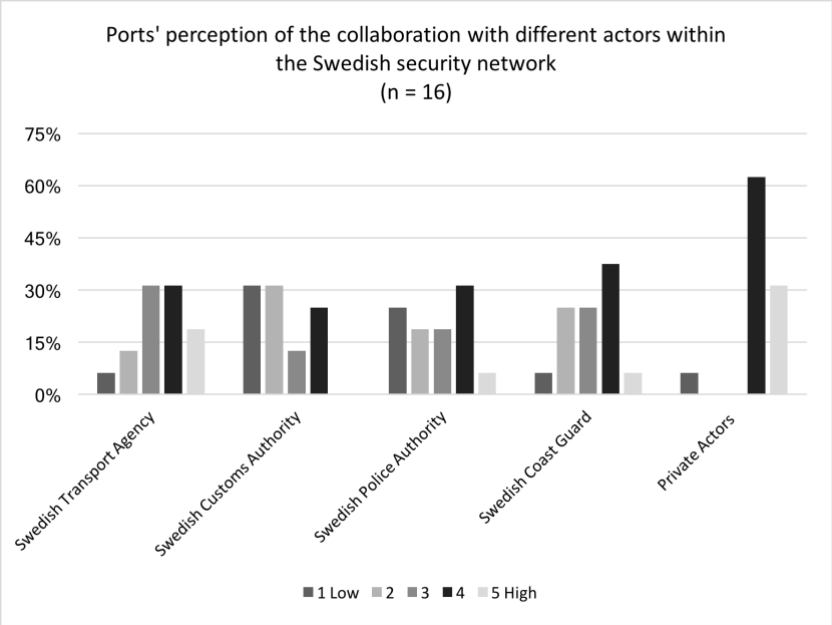

Figure 21: Perceived collaboration with actors of the Swedish security network

Since, figure 21 provides an overall result of the ports' perceptions of collaboration with different actors within the security network, further analysis was desirable. This was achieved by applying the same data used in figure 21 with figure 22. In this case, however, an average score for each individual actor/authority was calculated, where a line was drawn, representing the intermediate level between one and five, as seen below. The intension was to graphically assist the reader in identifying the result in relation to the intermediate level.

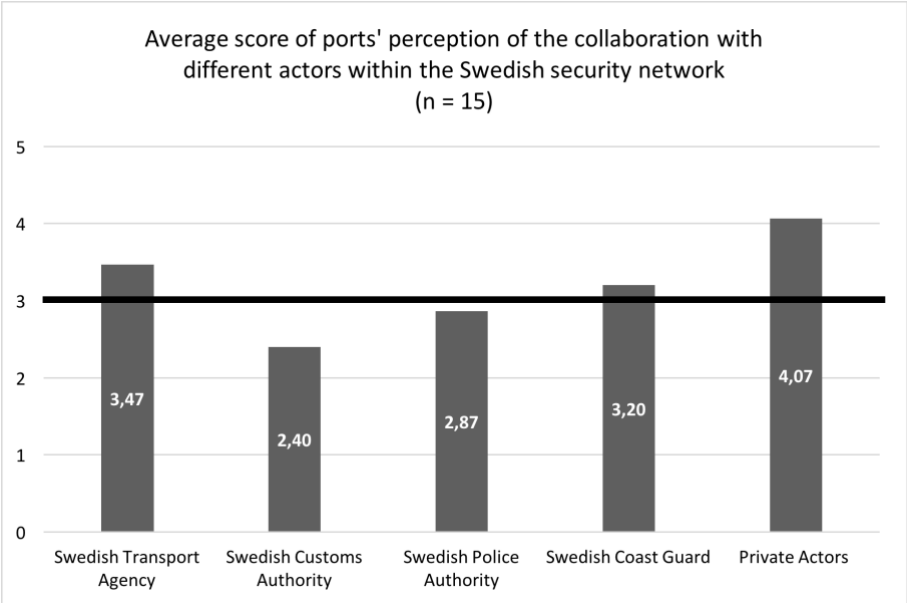

Figure 22: Average perceived collaboration with actors of the Swedish security network

Therefore, the results presented in figure 22 indicate that the ports in general perceive to have a good collaboration with the private actors. Furthermore, it also indicates that the Swedish Customs Agency (SCA) and Swedish Police Authority (SPA) are perceived by

the ports to have poor collaboration with the respondents. In addition, the respondents did not show a unified view on the collaboration with the Swedish Transport Agency (STA) and the Swedish Coast Guard (SCG). The STA and SCG scores were above the intermediate level, however, by less than half a point. The un-unified view of the collaboration is further strengthened in figure 21.

Furthermore, the STA were also asked to comment on the results presented in figure 21 and figure 22. Here, however, since the private actors have a business relationship with the ports, the STA were not surprised that the private actors scored the highest. Moreover, relative to the other authorities in the security network, the STA considers their score as rather good, since they are the only authority that is financed through fees. As stated by the STA:

> *"The STA considers that if one views the ranking in relation to the other three authorities; they are the only authority that charges for their surveys through an annual fee. Therefore; the result could be considered as quite good. The STA works with the aim that everything has a potential of being improved." - STA*

In this respect, to have a well-functioning security network in place is deemed as highly important for the security sector to function successfully in the ports by the interviewed respondents. Here, the security network is particularly important for smaller and medium-sized ports, since large ports have more expertise and an advantage in demanding more assistance from the authorities. Ports require assistance from those that carry large amounts of information and knowledge on the subject, as they themselves as operators cannot be expected to be experts within security. As stated by one respondent:

> *"The advantage with a security network is that one has an established organisation in the case that something occurs." - SA3*

Furthermore, another respondent stated:

> *"… it is really important that ports feel that there is a security network. Especially for the smaller and medium sized ports. They do not have the resources to have expert knowledge regarding the different regulations. To receive well-defined support from the authorities to be able to comply is really essential." - SA2*

Additionally, one respondent argued:

> *"I can only see advantages with a security network and with gathering as much competency as possible from as many perspectives as possible. The more perspectives the more balanced it becomes." - SA1*

Furthermore, information is both viewed, not only as important, but also sensitive within security networks by two respondents. If more actors are involved and information is distributed, the risk for sensitive information being leaked increases.

However, if the authorities require ports to comply with the regulations, the ports need to receive the relevant information to do so. As stated by one respondent:

> *"All matters in regards to security are classified, therefore the risk with a security network is the more actors that are involved, the greater the risk is of information being shared that shall not to be shared." - SA3*

Moreover, one respondent stated:

> *"If a port is to comply with all regulations they must receive input on how to act. They have to receive information concerning how a criminal looks today and what the real threats are. Otherwise they cannot do anything tangible. The critique from the ports about not receiving enough input from the authorities is simply correct." - LE*

The STA were questioned how they work with information-sharing in relation to security. They stated:

> *"The STA run campaigns within the maritime sector when new legal texts are adopted. Maritime security is a very small part of all the existing EU-regulations, directives, national laws, ordinances and regulations. Focus is given on new legal texts and it can be quite challenging enough to keep up to date with those." - STA*

Moreover, since the access to information is deemed vital, yet not readily available for the ports, the STA were asked how many inspectors they have that work within their organisation and how accessible they are to the ports in relation to interpreting regulations. They stated:

> *"The STA has three maritime security inspectors, where one works full time and two have other duties combined with port and port facilities inspections. […] Since the survey activities of the STA are financed through annual fees, it is in combination with inspections of various sorts that the ports are able to discuss issues with the inspectors." - STA*

Furthermore, related to information-sharing, the Swedish Police Authority (SPA) are considered to be a vital authority in sharing accurate information and ideally should be part of port security assessments. In addition, collaboration among ports and the SPA is something that the STA encourages. Nevertheless, according to the STA, the collaboration with the SPA varies, both concerning to which region in Sweden a port is located and the size of the port. As stated by the respondents:

> *"Obviously, it would be optimal if the police could be part of that process [port security assessment] as much as possible, however, that is not always the case." – STA*

"... The STA encourage that ports to a larger extent should have more contact [...] with the Swedish Police Authority. However, great variations are observed in different parts of Sweden." - STA

"In a larger maritime organisation, the ones responsible for security, most certainly have contacts at the police." - LE

Additionally, the Swedish Security Service (SÄPO) formerly had two agents who visited the ports and kept them informed on security related matters. However, this resource in no longer available according to one interviewee. In response to this statement, the STA informs that the Swedish Security Service (SÄPO) still actively works with port security. However, their work falls outside the scope of the STA since it is controlled by other legislations. As stated by the respondents:

"Previously there were resources within the Swedish Security Service, where two agents travelled around to ports and trained the management and personnel, however, that resource is not available anymore." - LE

Nevertheless, the STA clarifies that the SPA has undergone a major re-organisation in recent years, which is still affecting the organisation and how it functions. As stated by the STA:

"The SPA has undergone a re-organisation which is probably the largest one a Swedish authority has ever undergone. This contributes most probably to the challenges ahead for the SPA. Today, there are still areas that are not clear concerning how the organisation shall function in all parts of Sweden." - STA

The result presented in figure 22 could be to a disadvantage for the SPA, consideration has to be taken into account that the SPA have thoughtfully outsourced their day-to-day security work in ports to private security actors. The presence of private security guards, that now dominate the ports, can be viewed as an extended part of the SPA. The private security guards answer to, and are trained by, the SPA. As stated by one respondent:

"The SPA has chosen to allow the maritime industry to have private security actors that answer to the SPA and that the SPA has training and responsibility for according to Rikspolisstyrelsens regulation RPSFS 2009:21 and they are present. One could say that the component of the SPA that should have been visible in the ports is now instead represented by the maritime security guards." - LE

The SPA was asked to participate in the study and be interviewed regarding the results. However, they declined to partake and wished the study to note the reason for declining to answer any questions due to the current threat level. Nonetheless, the SPA recommended that the study instead reached out to the STA and ports to receive

answers to the questions, a measure that had already been completed by the time the SPA were asked to partake. However, the SPA should have been able to comment on certain aspects of the study without adventuring to reveal any confidential material. As stated by one interviewee:

> *"The SPA should be able to have opinions on the matter without for that sake risking to disclose any classified information."* - LE

Finally, the STA stated that they run campaigns when new regulations are introduced to inform concerned parties. However, they state that when the initial step of informing is completed, it is up the individual parties to ensure that they comply with the requirements.

> *"Information campaigns are run by the STA together with the implementation of new ordinances. After that initial step a process is underway and when everyone is familiar with the new requirements it is the individual's responsibility to follow them." – STA*

4.3 Security Culture

In the theoretical framework, it was concluded that an inadequate security culture, due to insufficient training and education in security awareness, can result in an increased exposure to security risks and threats. Thus, the surveyed ports were asked to grade their ability to share and distribute knowledge regarding security within their own organisation on a scale from one-to-five. One was the lowest possible ability to share and distribute knowledge regarding security in the organisation whereas five was the highest possible ability. The results of the survey are shown in figure 23 below.

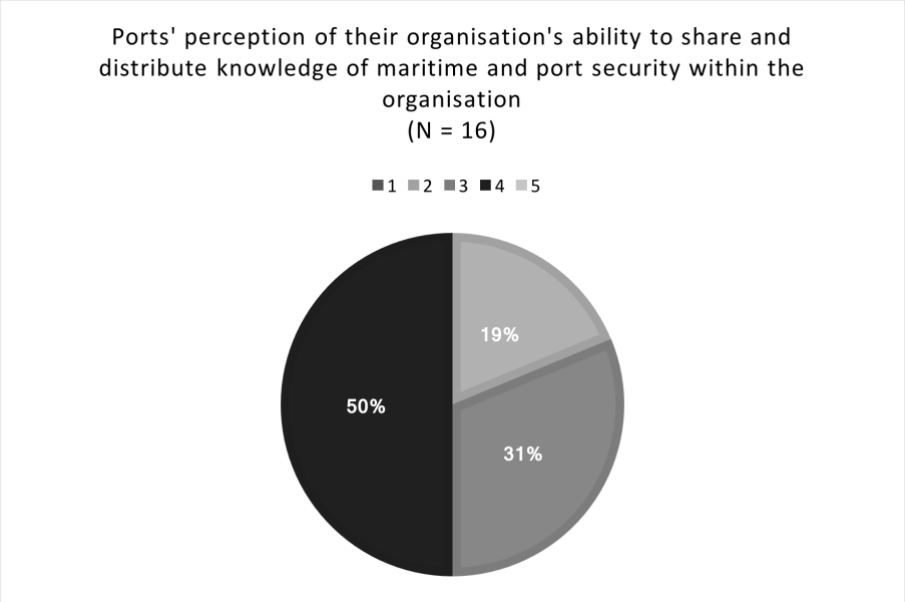

Figure 23: Perceived ability to share and distribute knowledge

The results signify that fifty percent of the surveyed ports viewed their ability to share and distribute knowledge as a four on the one-to-five scale. This indicates that they perceive themselves as being good at sharing knowledge, while still having the

possibility to improve up a step. In addition, it is significant to note that 19 percent of the surveyed ports rated their ability to share and distribute knowledge at level two on the scale. This suggests that almost one fifth of the ports perceive themselves as poor at sharing and distributing knowledge in regards to security.

Further, to analyse the result, the same data as used in figure 23 was applied in figure 24. However, in figure 24 the surveyed ports were divided into two categories, ports handling passengers and ports not handling passengers. This grouping was made since earlier in figures 8 and 11, passenger handling ports perceive themselves as better at complying with the regulations (figure 8) and having more available resources than non-passenger handling ports (figure 11).

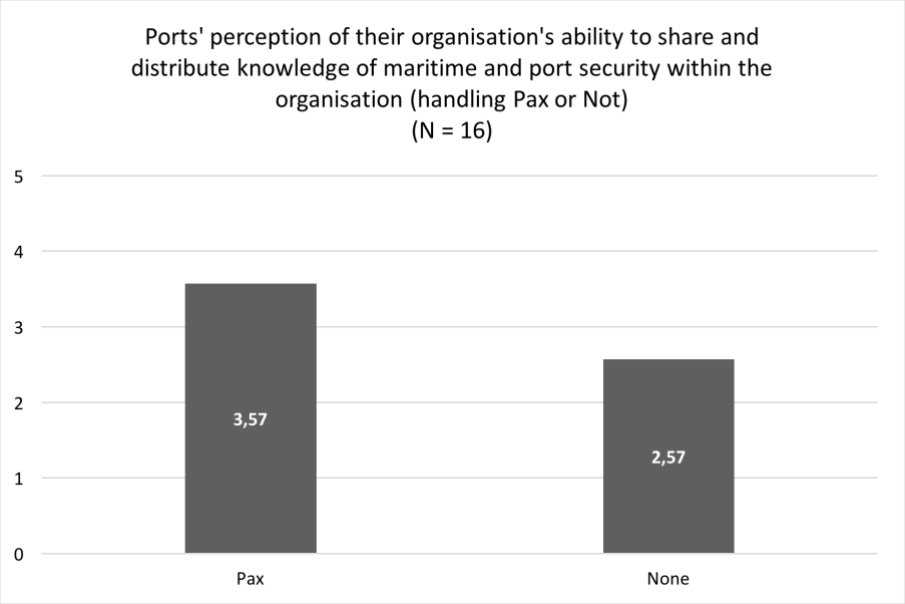

Figure 24: Perceived ability to share and distribute knowledge (pax or no pax)

Figure 24 indicates that passenger handling ports perceive they have a greater ability to share and distribute knowledge regarding maritime and port security regulations than ports that do not handle passengers. The result reveals that passenger ports on average rate themselves one full mark above non-passenger handling ports.

Moreover, all the interviewees highlighted the importance of having an established security culture in every port organisation. As stated by one respondent:

> *"It is really important to have a well-working security culture." - SA2*

However, one interviewee commented that security culture may be a well-functioning part of an organisation without the organisational calling it a "security culture".

> *"There are organisations that have a very well-functioning security culture, with both awareness and professionalism in everything they do, but they do not call it a security culture […]." – LE*

Furthermore, in order to establish a security culture in an organisation, a great deal of work is required. As one respondent stated, both the management and the customers must observe that the security culture within their organisation is a topic of discussion. Furthermore, an additional respondent stated that comprehending and reflecting security must reach all parts of the organisation for a culture to be established. The respondent further argued that access to information and tools to accommodate the information are key components when establishing a security culture.

> *"Both the management in an organisation and the customers have to remark that security culture is important. […] If security is never discussed, but other topics are, then we are going to compensate towards the direction of the topic raised instead." - SA2*

> *"To be able to reach a security culture or security environment, one must achieve the requirements of organisational culture and all that it brings to the table. That implies that all involved needs access to the same type of information and the same type of prerequisites to be able to embrace the information." - SA1*

Moreover, for ports to improve their security culture and find out if it is in place, the only possible way is after an unwanted incident. As stated by one respondents:

> *"I presume that what is required to reach any substantial improvements is a disaster. Looking at the actions that previously have been taken, they are all in the wake of catastrophes, the progressions so far are all reactive." – SA1*

This was further acknowledged by another respondent:

> *"It is hard to answer whether the security in place is ideal or not. It is not until something happens, god forbid, that one really can answer if that is the case. Therefore, it is important to, on a regular basis, conduct exercises, education and training." - SA3*

One respondent concluded that in order to establish a security culture, the work with security has to be something more than just trying to comply with regulations.

> *"One has to make it into something more than just compliance with regulations, because it is something more." - SA2*

Moreover, to be receptive to training and education, one must have the desire to learn. One must yearn for, and feel committed towards, undertaking security management in order to improve its effectiveness. As one respondent stated:

> *"You can only train those that have the capacity to be trained. The next step from a security management view is to say; you cannot work here with these things if you cannot gain the right competency and awareness skills. You have to be appropriate for the job." - LE*

4.4 Barriers towards regulatory compliance

At the end of the survey, the Swedish ports were asked an open-ended question regarding what barriers they experienced towards the compliance of maritime and port security regulations. The responses received were then divided into three main categories; [1] *regulations*; [2] *resources;* and; [3] *lack of support from the authorities*.

Two of the surveyed ports answered that they perceived the greatest barrier towards compliance as being the regulations themselves. Both of these ports argued that the current regulations appear to be composed to suit the ports with other prerequisites than they have. They believed that the regulations should take into consideration the individual flow of goods and activities in the various ports.

Furthermore, five ports claimed that resources are the greatest barrier towards compliance. Three of these five ports specifically claim that they lack both finances and personnel to fully comply. One port stated that more financial resources could assist them in recruiting advisers and technical equipment. Two other ports stated that knowledge is the greatest barrier, while another exemplified this by claiming that the lack of knowledge and the lack of education and training materials results in difficulties in conducting proper security drills.

In addition, four of the surveyed ports claimed that the authorities were acting as the greatest barrier. Here, it was stated, both a lack of explicit information and a lack of available resources, combined with inactivity from the STA, are the greatest barriers. One port wished for the many ambiguous interpretations, which are possible in the regulations, to be addressed by the STA by assisting and guiding the ports more in their security work, while one other port expressed a desire for the SPA to be more supportive.

Additionally, at the end of each conducted interview, the respondents were asked what they believed to be the greatest barrier for Swedish ports towards the compliance of maritime and port security regulations. One of the interviewees advocated the need for a certain level of acceptance towards the stipulated regulations for maritime and port security as the greatest barrier towards compliance. Here, comprehending the reasons behind the regulations' existence, structure and intention is clearly of great importance. The security regulations currently in force will become obsolete if port organisations are reluctant to accept that there is a threat. Security will be a matter of doing as little as possible in order to become approved by an inspector and not about protection. As stated by the respondent:

> *"The reason for working with security has to be based on the very reason that security regulations exist and not what one is compelled to do." - SA1*

> *"… the ports have to ransack themselves and be reminded of why the regulations are in place, because that is going to fade with time and result in the regulations only being instrumental and compliance only something that needs to be achieved without a proper reason." - SA1*

> *"... the greatest barrier towards compliance boils down to the acceptance of a threat scenario. As long as we do not accept that there is a threat, we will not take the [ISPS] Code seriously. If we do not take the [ISPS] Code seriously it will never be good. In that case one will only do as little as possible to be approved by the inspector." - SA1*

Furthermore, one respondent stated that the greatest barrier towards compliance is resource availability. The ports need more time and money in order to improve their security work. However, more resources will only be available to the ports as a reaction to the industry being exposed to a serious threat or incident.

> *"Time and money, and to get that, a larger incident that nobody wants is required." - SA 2*

Moreover, knowledge-creation and information-sharing were considered as essential aspects to successfully comply with security regulations according to one interviewee. However, in order to establish an effective security environment within an organisation, information-sharing and transparency are required. Unless this is achieved, knowledge cannot be created, and without knowledge-creation, security awareness is unreachable.

> *"There are incredibly high demands on knowledge, regardless of where in the organisation you are. Everyone does not have the advantage to work with security, so the greatest barrier towards compliance is to receive information." - LE*

Finally, there could be a lack of comprehension from Swedish ports in understanding that the European Commission (EC) is the main responsible authority for maritime security within the European Union (EU). Therefore, it is also accountable for governing the overall maritime security regime. As stated by the STA:

> *"... not all ports realise that the EC are in full control of the overall maritime security matters within the EU. The EC, through their maritime security inspections of its member states, assures that the level of security is acceptable and even." - STA*

4.5 Summary of main empirical and analytical result

In the following section, the main empirical and analytical result identified from the collected data are summarised in the table below (*Table 4*).

Table 4: Main empirical and analytical result

Main empirical and analytical result	
Regulatory framework	• Port organisations operate in a global environment together with international competition and governance control. Hence, ports prioritise compliance towards the global and international regulations in order to be market competitive. Consequently, it is evident that there is a lack of knowledge and understanding of the national security regulations and thus difficult to comply with for Swedish ports. • It is believed that public security awareness creates a public opinion which influences the passenger ports to undertake more efficient and comprehensive security. Furthermore, it is suggested that passenger ports can use security as a competitive advantage and thus can allocate more resources for security as it is regarded as a revenue-related activity. • Since legal compliance is a must to trade, port organisations at least will strive towards minimum regulatory compliance. However, commercial interests do not necessarily conform with security standards and guidelines. Subsequently, port organisations with limited resources may give priority to apparent revenue-related activities instead of focusing on security improvements. • Smaller ports in Sweden express a desire for the security regulations to be more locally adapted. Global security regulations are a necessity to ensure that the entire supply chain is intact. The current security regulations request ports to conduct their own risk assessment Subsequently, the regulations allow for certain local variation within their boundaries. However, ports may lack the knowledge and resources to utilise this possibility. • More explicit tools and methods for implementing global and international security regulations should be made available according to the smaller ports in Sweden. It is believed that this desire derives as a consequence due to the lack of resources. More explicit tools and methods are believed to facilitate the implementation and require less means. However, it is considered that the individual Member States of the IMO and EU should support the industry so as to successfully comply with the regulations.
Security network	• A well-functioning security network is deemed important and can work as a source of expertise while increasing security awareness. Further, within the security network, information and knowledge can be elaborated and shared across organisations. • Security information is sensitive and often classified and is thus not made readily available. However, inadequate transparency within the security network may result in a lack of important security information being shared among the actors. Consequently, this could suggest that the ports do not receive relevant, and maybe vital information, with regard to their security.

Security culture	• An established security culture, at all levels of the organisation, is considered to be an essential element for a port to successfully achieve efficient security. • Information availability and transparency regarding security within an organisation, are suggested to be important prerequisites to improve efficiency. Managers and external customers must be involved and committed in motivating and engaging all members of an organisation in the security work.

5 DISCUSSION

This chapter presents the discussion of the result and analysis revealed in chapter four. Further, the validity and generalisation of the thesis is discussed.

The theoretical framework of this thesis has established that the current regulations for maritime and port security are complex. The result shows that a Swedish port is obliged to comply with a total of nine security legislations which exist at the global, international and national levels. However, as identified in this study, the regulatory framework is considered to be substantial if the actors involved fully contribute and comply.

Furthermore, the study has identified that Swedish ports, in general, perceive they have insufficient resources to successfully develop and implement organisational security measures. However, this study does not advocate that the solution towards more efficient port security is more time, money or personnel. Instead, the study identifies that in order for all the actors involved in maritime and port security to successfully comply with the above-stated complex regulations, "knowledge-creation" and "information-sharing" are the most important.

In addition, the two most important concepts, knowledge-creation and information-sharing, have to take place at two levels. To begin, the actors of the Swedish security network must establish an inter-organisational sharing of information and become more transparent. Clearly, security information is sensitive, however, the well-founded belief is still that areas of security can be distributed without risking the security of the public. Here, increasing and refining the information shared by the Swedish Transport Agency and Swedish Police Authority, could motivate and enlighten the port organisations to improve their security. Further, port organisations must understand their responsibility and take the actions necessary to develop and improve the security environment, since they are an important part of it. The essence of an enhanced security network is through collaboration between both the private and governmental actors.

Moreover, as the result shows, Swedish ports perceive that they can improve their knowledge-creation and information-sharing on an intra-organisational level. To accomplish this, is deemed vital by the research for a more efficient port security outcome. Here, the information shared within the security network must be filtered through the entirety of all the port organisations to ensure that a rigid and efficient security culture is evident in the ports.

In summary, the current regulatory security framework is sound, however it requires that all the parties are actively involved; and for all the parties to be actively involved, the knowledge-creation and information-sharing must be significantly improved at both the inter- and intra-organisational levels. If successfully managed and organised a sustainable development of the port security environment in Sweden can be achieved.

5.1 Validity of the result

In order to obtain the necessary information required for this research, a deductive case study has been conducted. The findings identified in the theoretical framework have been used to develop relevant questions for the survey. In total, 16 Swedish public ports

participated in the survey and thereby contributed with data. Since there are a total of 34 public ports organisations in Sweden that fulfilled the prerequisites to participate in the study, the empirical data from the survey does not necessarily reflect the general perspective of the industry. This could have been avoided by increasing the number of participants which would then have resulted in an increased validity for the study. To further enhance the validity, supplementary studies from other Member States of the IMO and EU, may be needed.

Moreover, some of the ports that were asked to participate declined to contribute with a given reason. Since the survey included questions concerning security, several ports declined to participate because they have a policy not to discuss matters that regard security with people outside of the organisation who have not been vetted. Furthermore, two ports declined to participate because they believed that they did not have the knowledge to answer the survey fairly. Nevertheless, among the participating ports, 71,4 percent of the major public port organisations, 62,5 percent of major Swedish passenger ports and 47 percent of all public port organisations in Sweden, have contributed with data. In addition, the port representatives who responded to the survey, were all actively working with port security. Hence, this has considerably increases the validity of the research outcome.

Furthermore, the collected data from the survey was used as a basis for formulating the open-ended questions for the interviews. In order to increase the knowledge in the field of the study while gaining valuable information, in-depth interviews were targeted and executed by engaging key informants. In total, five interviews were conducted of which four were with experts in the field of the studied research. Moreover, one interview was conducted with a spokesperson from the Swedish Transport Agency. Furthermore, the industry and employers' organisation Ports of Sweden (PoS) was asked to participate. However, after communicating with the PoS and stating the purpose of the study, they did not respond with a suitable candidate to be interviewed.

Since there is a risk of being biased when formulating questions and conducting interviews, the time-period for analysing the result was extensive. This was conducted to allow for personal reflections and evaluating aspects that could influence the result of the interviews. Moreover, to avoid preconceptions and misinterpretations in the data collected from the interviews, the citations were verified by each of the respondents after the interviews. These undertakings were performed in order to increase the validity of the study.

In addition, the diverse sources of evidence used to gather the relevant data, allowed for a cross-analysis of the result, which in turn increased its the internal validity. Further, in order to ensure the satisfactory outcome of the triangulation and internal validity of the study, a theoretical framework, surveys and interviews were all used as methods of the data collection.

5.2 Generalisation

The review process of previously published research did not identify any earlier publications which covered the area of the study. Therefore, it is considered that the

findings from this Master's thesis can be a valid contribution for existing and future research within the scope of maritime and port security.

Moreover, this study can be applied at various regulatory levels to other Members States of both the European Union (EU) and the International Maritime Organization (IMO). This is significant as the maritime port sector is an international industry with governance control and regulatory frameworks at the EU and IMO level that all ports and port facilities must comply with. However, it is concluded that the governance control and regulatory framework on a national level might differ significantly among the many Member States. Therefore, if the result is to be used in other settings, consideration must be taken regarding the national regulations of the States they are to be adopted in. Hence, the result may not be applicable, and not necessarily reflect, the reality of port organisations outside Sweden.

Furthermore, the method used for this study can be replicated by other researchers in order to comprehend the regulatory security environment for port organisations. Nevertheless, there is a need for consideration with regards to the specific conditions facing the port organisations studied. For example, adjustments to the framework may be required to manage the specific environment of the ports researched. In addition, security is a complex issue and there might be several factors that could influence the maritime and port security environment. Therefore, it could be argued that this research study does not cover all the relevant aspects which might influence a port organisation's ability to comply with the regulatory security framework. However, the result and analysis presented give an indication in the studied area as to which barriers exist for Swedish ports to comply with the regulatory security framework. This thesis could thus be used as a benchmark study for further research that results in substantially improving effective port security.

6 CONCLUSION

This chapter summarises the answers to the stated research questions. Furthermore, the theoretical contributions, practical implications and further research are discussed. Finally, the concluding statement of the thesis is given.

The purpose of this research is two-fold; [1] to present a theoretical framework for the evaluation of the regulatory framework for maritime and port security at the global, international and national levels, and [2] to identify barriers in the legal compliance of the regulatory security framework for Swedish port organisations.

- What are the main barriers that limit Swedish port organisations' abilities to successfully comply with the regulatory framework for maritime and port security at the global, international and national levels?

The study concludes that barriers exist which limit the Swedish port organisations' abilities to successfully comply with the regulatory framework for maritime and port security at the global, international and national levels. The three main barriers identified by the study are; [1] *the inadequate knowledge and understanding of the regulatory security framework;* [2] *the lack of security subject to prioritised commercial interests and limited resource availability;* and*;* [3] *the insufficient collaboration and support within the security network.*

- How does knowledge-creation and information-sharing correlate with Swedish port organisations' abilities to successfully comply with the regulatory framework for maritime and port security at the global, international and national levels?

Moreover, the study concludes that knowledge-creation and information-sharing correlate with the Swedish port organisations' abilities to successfully comply with the regulatory framework for maritime and port security at the global, international and national levels. The regulatory framework was identified as a complex system of different legislations by the theoretical framework. Moreover, the thesis concludes that there are limitations in knowledge and understanding of the contextual relationship between the regulatory framework and security. The stated limitations ultimately influence upon a Swedish port's ability to successfully develop and implement measures that result in a satisfactory and effective port security environment. Here, transparency and the sharing of information regarding security at the inter- and intra-organisational levels are required in order to establish a vigorous security environment. Thus, the study concludes that both security network and security culture are important components, which can either facilitate or limit the processes of knowledge-creation and information-sharing. Therefore, if the sharing of information is successfully managed and organised, security knowledge can be created and established, both vertically and horizontally within the system. Consequently, this will increase, improve and ensure a sustainable development of security, not only for the individual port organisation but also for the entire maritime and port industry.

The researchers of this thesis regard knowledge-creation and information-sharing as the most significant leverage points. The authors conclude that the main identified barriers

can be limited and mitigated by successfully emphasizing and managing these aspects. Unless achieved, port security will be a matter of minimum compliance towards the regulatory security framework, and not a matter of protecting the individual port, and in extension the entire system.

Furthermore, the result and conclusion of this study does not necessarily replicate a definite reality. Nevertheless, the research conducted can assist in explaining how the Swedish maritime and port security structure functions. Furthermore, the study contributes in illustrating how the actors of the Swedish security network collaborate.

The maritime industry is a major pillar for globalisation and is necessary for international trade to continue and thrive. Simultaneously, increasing conflicts, political disturbance and criminal activities have forced the world to re-shape and engage in the way that security and risk assessments are now viewed and executed. A potential breach in port security can result in huge negative impacts, financial, societal and environmental, not only to a single nation but also internationally. In order to improve security and protect the entire system, it is essential to increase the significance of maritime and port security. Here, all the actors involved in security must understand its strategic importance and be willing to partake. They must evoke common actions and share responsibilities for a continuously sustainable development of a secure port industry. The question should be asked; does the world need another 9/11 to ensure security, or can the maritime industry be proactive instead rather than following its usual footsteps of reactiveness?

6.1 Theoretical contributions

The research conducted herein is the only identified study to focus on the Swedish port's perception towards the current regulations for maritime and port security. Moreover, it is the only identified research conducted of its kind at the national, international and global levels. Thus, it is considered that the study has not exhausted the subject area, but instead can serve as a starting point for further research.

In addition, to the authors' knowledge, the study is the first research to apply the embedded units of analysis of knowledge-creation and information-sharing to the port compliance of security regulations. Previously published identified research has focused on financial aspects for the implementation of security regulations and harmonisation of training and education for security in ports. In general, very few publications related to the ports perception of barriers towards compliance have been identified, thus further studies are required that focus on the matter.

6.2 Practical implications

The main practical implication acknowledged by the research is that actors within the security network receive awareness regarding the conclusion that barriers exist for Swedish ports to comply to the current security regulations. The first step in ensuring that necessary actions are taken to limit and mitigate the barriers, is an increased awareness and understanding of them among the security actors.

Furthermore, the researchers of this thesis recommend the second step in order to eliminate the existing barriers, should be to substantially increase knowledge and

information among the ports. The State is responsible for overall protection; however, it lacks the capacity to ensure this and therefore requires the industry's assistance. The Swedish Transport Agency is financed through annual fees; therefore it is not considered as the main responsible party. Instead, the conclusion is that the Swedish Police Authority should create a division that solely and continuously works closely with the ports concerning security. Through the proposed new division, the ports should have a close relationship and be constantly updated and informed. The cost for such a division with for example, two or three fulltime employees, is considered as reasonable compared to the potential costs of any lack in security compliance. The suggestions to eliminate the existing barriers should thus be regarded as an inexpensive investment, and not as an increased cost.

6.3 Further research

When conducting this study, the researchers have identified several areas that could be further examined, both to elaborate the results of the research, and also to further elaborate the current knowledge and understanding of port security from a social science perspective.

Firstly, a recommendation is made to study security accidents and near-miss reports. Gathering report-data from the ports would then allow researchers to further assess the compliance and compare it to the result of this study, and data regarding financial and personnel resources could simultaneously be collected and analysed. Secondly, further research is recommended that allows for the time spent at the ports. Unstructured interviews concerning security could then be continually conducted with the employees at all levels of the port organisation in their natural work-environment. This approach permits for an examination of the security culture, knowledge-creation and information to be shared within the port organisation. Finally, the method used in this study could be applied for additional research in States other than Sweden, and for an international study on port organisations. This would allow for local variations and international parallels to be identified and compared.

REFERENCES

Allen, N. H. (2006). The Container Security Initiative costs, implications and relevance to developing countries. *Public Administration and Development,* vol. 26**,** no. 5, pp. 439-447.

Alvesson, M. (2002) *Understanding organizational culture.* London: Sage Publications Ltd.

Andritsos, F. (2013) *Port security & access control: A systemic approach*. Information Intelligence Systems and Applications (IISA) 2013 Fourth International Conference, Piraeus, Greece. IEEE.

Andritsos, F. & Mosconi, M. (2011) *Port security in EU: A systemic approach*. Waterside Security Conference (WSS), 2010 International, Carrara, Italy. IEEE.

Argote, L. (2013) *Organizational Learning - Creating, Retaining and Transferring Knowledge.* 2nd. ed. New York: Springer Science + Business Media.

Argote, L. & Miron-Spektor, E. (2011). Organizational Learning: From Experience to Knowledge. *Organization Science,* vol. 22**,** no. 5, pp. 1123-1137.

Australian Government (2018) *A guide to developing and implementing a Suspicious Activity Identification Program at ports*. http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/INFRA2702_OTS_MARITIME_ACTIVITY_SUSPICIOUS_ACTIVITY_FA.pdf (26 Feb, 2018).

Berta, W., Cranley, L., Dearing, J. W., Dogherty, E. J., Squires, J. E. & Estabrooks, C. A. (2015). Why (we think) facilitation works: insights from organizational learning theory. *Implementation science,* vol. 10**,** no. 1, pp. 1-14.

Bichou, K. (2004). The ISPS Code and The Cost of Port Compliance: An Initial Logistics and Supply Chain Framework for Port Security Assessment and Management. *Maritime Economics & Logistics,* vol. 6**,** no. 4, pp. 322-348.

Brewer, R. (2014) *Policing the waterfront: networks, partnerships and the governance of port security.* Oxford: Oxford University Press.

Bryman, A. & Bell, E. (2015) *Business Research Methods.* 4th. ed. Oxford: Oxford University Press Inc.

Bueger, C. (2015). What is maritime security? *Marine Policy,* vol. 53**,** no. 1, pp. 159-164.

Burns, M. G. (2013). Estimating the impact of maritime security: financial tradeoffs between security and efficiency. *Journal of Transportation Security,* vol. 6**,** no. 4, pp. 329-338.

Chapsos, I. & Kitchen, C. (2015) *Strengthening Maritime Security Through Cooperation.* Amseterdam: IOS Press BV.

Christopher, K. (2014) *Port security management.* Second Edition. Boca Raton: CRC Press.

Council of the European Union (2014) *European Union Maritime Security Strategy*. Brussels: Council of the European Union. (11205/14).

Dai, Z. (2012). Toward a learning-based view of innovation. *Competitiveness Review: An International Business Journal,* vol. 22**,** no. 1, pp. 18-27.

Denscombe, M. (2014) *The good research guide - For small scale research projects.* 5th ed. Maidenhead, England: Open University Press.

Directive 2005/65/EC. *On enhancing port security.* Brussels, European Commission.

Dupont, B. (2004). Security in the age of networks. *Policing & Society,* vol. 14**,** no. 1, pp. 76-91.
Easterby-Smith, M., Thorpe, R. & Jackson, P. R. (2015) *Management and business research.* 5th ed. London, UK: SAGE.
Ebers, M. (1997) *The Formation of Inter-Organizational Networks.* New York: Oxford University Press.
Eddy, E. R., D'Abate, C. P., Tannenbaum, S. I., Givens-Skeaton, S. & Robinson, G. (2006). Key Characteristics of Effective and Ineffective Developmental Interactions. *Human Resource Development Quarterly,* vol. 17**,** no. 1, pp. 59-84.
Edgerton, M. (2013) *A Practitioner's Guide to Effective Martitme and Port Security.* Hoboken, New Jersey: John Wiley & Sons, Inc.
Eklöf Amirell, S. (2016). Global maritime security studies: The rise of a geopolitical area of policy and research. *Security Journal,* vol. 29**,** no. 2, pp. 276-289.
Ekow, M. M. (2011) *Maritime Risk and Organizational Learning.* Farnham, United Kingdom: Ashgate Publishing Limited.
Ekwall, D. & Rolandsson, B. (2013). Security aspects on corporate culture in a logistics terminal setting. *Journal of Transportation Security,* vol. 6**,** no. 1, pp. 13-25.
Eski, Y. (2016). The war on meaninglessness: A counter-terrorist self through an absent terrorist other. *Ethnography,* vol. 17**,** no. 4, pp. 460-479.
EUR-Lex (2016) *Security for ships and port facilities*.
European Commission (2018a) *Maritime Security*. https://ec.europa.eu/transport/modes/maritime/security_en (5 March, 2018).
European Union (2018) *Regulations, Directives and other acts*. https://europa.eu/european-union/eu-law/legal-acts_en (5 March, 2018).
Farrell, S. (2001). If it ain't bust, don't fix it: the proposed EU directive on market access to port services. *Maritime Policy & Management,* vol. 28**,** no. 3, pp. 307-313.
Flynn, M., Lee, P. T.-W. & Notteboom, T. E. (2011) The next step on the port generations ladder: Customer-centric and community port *In:* Notteboom, T. E. (ed.) *Current issues in shipping, ports and logistics.* Brussels, Switzerland: Academic and Scientific Publishers.
Germond, B. (2015). The geopolitical dimension of maritime security. *Marine Policy,* vol. 54**,** no. 1, pp. 137-142.
Gill, P. (2006). Not Just Joining the Dots But Crossing the Borders and Bridging the Voids: Constructing Security Networks after 11 September 2001. *Policing & Society,* vol. 16**,** no. 1, pp. 27-49.
Harrell, M. C. & Bradley, M. A. (2009) *Data Collection Methods: Semi-Structured Interviews and Focus Groups*. Santa Monica, California: RAND Corporation. (W74V8H-06-C-0002).
Hellberg, P. (2009). *Effects of the ISPS Code on ship and port security.* Master of Science, World Maritime University.
Helmick, J. S. (2008). Port and maritime security: A research perspective. *Journal of Transportation Security,* vol. 1**,** no. 1, pp. 15-28.
Hopkin, P. (2014) *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management.* London, Philadelphia: Kogan Page.
Hyde, K. F. (2000). Recognising deductive processes in qualitative research. *Qualitative Market Research: An International Journal,* vol. 3**,** no. 2, pp. 82-90.
International Chamber of Shipping (2017) *Shipping and World Trade*. http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade (8 February, 2018).

International Maritime Organization. *Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation.* London, UK,
International Maritime Organization (2003) *International Ship and Port Facility Security (ISPS) Code.* London, UK.
International Maritime Organization (2017) *SOLAS XI-2 and the ISPS Code*. http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/solas-xi-2%20isps%20code.aspx (18 April, 2017).
International Maritime Organization (2018a) *Maritime Safety*. http://www.imo.org/en/OurWork/Safety/Pages/Default.aspx (8 March 2018, 2018).
International Maritime Organization (2018b) *Guide to Maritime Security*. http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Default.aspx (10 February, 2018).
International Maritime Organization (n.d.) *Guide to Maritime Security*.
Johannesson, P. & Perjons, E. (2014) *An Introduction to Design Science.* Cham: Springer International Publishing.
Kelley, K., Clark, B., Brown, V. & Sitzia, J. (2003). Good practice in the conduct and reporting of survey research. *International Journal for Quality in Health Care,* vol. 15**,** no. 3, pp. 261-266.
Kenneth, C. (2015) *Port Security Management.* 2nd ed. Florida: Taylor & Francis Group.
Ketokivi, M. & Choi, T. (2014). Renaissance of case research as a scientific method. *Journal of Operations Management,* vol. 32**,** no. 5, pp. 232-240.
Kvale, S. (2007) *Doing interviews.* Thousand Oaks, California: SAGE Publications.
Kvale, S. & Brinkmann, S. (2009) *InterViews: Learning the Craft of Qualitative ResearchInterviewing.* Los Angeles, CA: Sage.
LaPorte, T. & Consolini, P. M. (1991). Working in practice but not in theory: theoretical challenges of "High-Reliability Organizations". *Journal of Public Administration Research and Theory,* vol. 1**,** no. 1, pp. 19-47.
Linnenluecke, M. K. & Griffiths, A. (2010). Corporate sustainability and organizational culture. *Journal of World Business,* vol. 45**,** no. 4, pp. 357-366.
Liwång, H., Sörenson, K. & Österman, C. (2015). Ship security challenges in high-risk areas: manageable or insurmountable? *WMU Journal of Maritime Affairs,* vol. 14**,** no. 2, pp. 201-217.
Malcolm, J. A. (2016). Responding to international terrorism: The securitisation of the United Kingdom's ports. *The British Journal of Politics and International Relations,* vol. 18**,** no. 2, pp. 443-462.
Maritime Forum (2013) *Hamnverksamhet*. https://maritimeforum.se/sjofart/hamnen/#.WoKpiWaZOCQ (13 February 2018, 2018).
Martins, E. C. & Terblanche, F. (2003). Building organisational culture that stimulates creativity and innovation. *European Journal of Innovation Management,* vol. 6**,** no. 1, pp. 64-74.
Mazaheri, A. & Ekwall, D. (2009). Impacts of the ISPS code on port activities: a case study on Swedish ports. *World Review of Intermodal Transportation Research,* vol. 2**,** no. 4, pp. 326-342.
Metaparti, P. (2010). Rhetoric, rationality and reality in post-9/11 maritime security. *Maritime Policy & Management,* vol. 37**,** no. 7, pp. 723-736.

Mileski, J., Mejia, M. & Ferrell, T. (2015). Making lemonade out of lemons: port operators' perceptions of their port security regulation compliance. *WMU Journal of Maritime Affairs,* vol. 14**,** no. 1, pp. 93-108.
Mitchell, R. & Boyle, B. (2010). Knowledge creation measurement methods. *Journal of Knowledge Management,* vol. 14**,** no. 1, pp. 67-82.
Notisum (n.d.) *Lagar, förordningar och föreskrifter hänger ihop*. http://www.notisum.com/News.aspx?itemid=5478 (7 March, 2018).
Notteboom, T. (2011) *Current issues in shipping, ports and logistics.* Brussels, Belgium: Uitgeverij UPA University Press.
O'Toole, L. J. (1997). Treating networks seriously: Practical and research-based agendas in public administration. *Public Administration Review,* vol. 57**,** no. 1, pp. 45-52.
Opdenakker, R. (2006). Advantages and disadvantages of four interview techniques in qualitative research. *Forum: Qualitive Social Research,* vol. 7**,** no. 4, pp. 1-9.
Page, B. I. & Shapiro, R. Y. (1983). Effects of Public Opinion on Policy. *American Political Science Review,* vol. 77**,** no. 1, pp. 175-190.
Papa, P. (2012). US and EU strategies for maritime transport security: A comparative perspective. *Transport Policy,* vol. 28**,** no. pp. Transport Policy.
Papa, P. (2013). US and EU strategies for maritime transport security: A comparative perspective. *Transport Policy,* vol. 28**,** no. 1, pp. Transport Policy.
Pietersen, C. (2017). Organizational culture: a foundational perspective. *African Journal of Economic and Management,* vol. 8**,** no. 3, pp. 262-273.
Piétre-Cambacédès, L. & Chaudet, C. (2010). The SEMA referential framework: Avoiding ambiguities in the terms "security" and "safety". *International Journal of Critical Infrastructure Protection,* vol. 3**,** no. 2, pp. 55-66.
Regulation EC 725/2004. *On enhancing ship and port facility security.* Brussels, European Commission.
Roberts, K. H., Bea, R. & Bartles, D. L. (2001). Must accidents happen? Lessons from high-reliability organizations. *Academy of Management Executive,* vol. 15**,** no. 3, pp. 70-80.
Roe, M. (2009). Multi-level and polycentric governance: effective policymaking for shipping. *Maritime Policy & Management,* vol. 36**,** no. 1, pp. 39-56.
Roe, M. (2013) *Maritime Governance and Policy-Making.* London: Springer-Verlag.
Roer, K. (2015) *Build a Security Culture.* Cambridgeshire, United Kingdom: IT Governance Publishing.
Romero-Faza, D. & Camarero-Orive, A. (2017). Risk assessment of critical infrastructures - New parameters for commercial ports. *International Journal of Critical Infrastructure Protection,* vol. 18**,** no. 1, pp. 50-57.
Sadovaya, E. & Thai, V. V. (2016). The Effective Maritime Security Management Model (EMSMM): A perspective from practitioners in Singapore. *Security Journal,* vol. 29**,** no. 4, pp. 661-682.
SafeSeas (2018) *Mastering Maritime Security. Reflexive Capacity Building and the Western Indian Ocean Experience*. Cardiff, UK: SafeSeas.
Saunders, M., Lewis, P. & Thornhill, A. (2016) *Research methods for business students.* Harlow: Pearson Education.
SFS 2004:283. *Om sjöfarsskydd.* Stockholm, Swedish Government.
SFS 2004:487. *Om sjöfartsskydd.* Stockholm, Swedish Government
SFS 2006:1209. *Om hamnskydd.* Stockholm, Swedish Riksdag.

SFS 2006:1213. *Om hamnskydd.* Stockholm, Swedish Government.
SFS 2008:1152. *Om sjöfartsskydd.* Stockholm, Swedish Government.
Sjöfartsverket (1999) *Projekt HSS: Strategisk analys, underlag till SAMPLAN om hamnstruktur och sjöfart*.
SJÖFS 2004:13. *Om sjöfarsskydd.* Norrköping, Swedish Maritime Administration.
SJÖFS 2007:1. *Om hamnskydd.* Norrköping, Swedish Maritime Administration.
SJÖFS 2013:4. *Sjöfartsverkets tillkännagivande av register över allmänna farleder och allmänna hamnar*. Norrköping, Swedish Maritime Administration.
Spens, K. M. & Kovács, G. (2006). A content analysis of research approaches in logistics research. *International Journal of Physical Distribution & Logistics Management*, vol. 36**,** no. 5, pp. 374-390.
Sveriges Hamnar (2016) *Trafiken i Sveriges hamnars medlemsföretag*. https://www.transportforetagen.se/ForbundContainer/Svenska-hamnar/Branschfragor/Hamnstatistik/Hamnstatistik/ (13 February 2018,
Swedish Maritime Administration (n.d.) *Maritime Security/Port Security*. https://transportstyrelsen.se/en/shipping/Ship-traffic/Maritime-SecurityPort-Security/ (15 January, 2018).
Swedish Riksdag (2005) *Sjöfartsskydd*. Stockholm, Sweden: Riksdagstryckeriet. (2005/06:RFR7).
Swedish Riksdag (n.d.) *EU:s lagar och regler - EU-lag går före svensk lag*. http://eu.riksdagen.se/vad-gor-eu/en-eu-lag-blir-till/eus-lagar-och-regler/# (7 March, 2018).
Swedish Transport Agency (n.d. a) *Maritime Security/Port Security*. https://transportstyrelsen.se/en/shipping/Ship-traffic/Maritime-SecurityPort-Security/ (15 January, 2018).
Swedish Transport Agency (n.d. b) *Tillsyn*. https://www.transportstyrelsen.se/sv/sjofart/Fartyg/Tillsyn/ (9 March, 2018).
Thai, V. V. (2007). Impacts of Security Improvements on Service Quality in Maritime Transport: An Empirical Study of Vietnam. *Maritime Economics & Logistics*, vol. 9**,** no. 4, pp. 335-356.
Thai, V. V. (2009). Effective maritime security: conceptual model and empirical evidence. *Maritime Policy & Management*, vol. 36**,** no. 2, pp. 147-163.
Thai, V. V. & Grewal, D. (2007). The Maritime Security Management System: Perceptions of the International Shipping Community. *Maritime Economics & Logistics*, vol. 9**,** no. 2, pp. 119-137.
The European code of conduct for research intregrity (2017) *The European Code of Conduct for Research Intregrity*. Berlin, Germany: All European Academies.
Trafikanalys (2017) *Shipping goods 2016*. Stockholm, Sweden: Sveriges officiella statistik. (2017:19).
Transportföretagen (n.d.) *Sjöfartsskydd*. https://www.transportforetagen.se/ForbundContainer/Svenska-hamnar/Branschfragor/Miljo-arbetsmiljo-och-sakerhetskydd/Sakerhet/Sjofarts-och-hamnskydd/Sjofartsskydd/ (5 March, 2018).
Trelawny, C. (2005) *Maritime Security: Implementation of the ISPS Code*. 3rd Intermodal Africa 2005 Tanzania Exhibition and Conference, Dar es Salaam.
United Nations (2008) *Oceans and the law of the sea. Report of the Secretary-General, UN General Assembly*. New York: United Nations: United Nations. (Document A/63/63).

Urciuoli, L., Ekwall, D. & Torstensson, H. (2013). Achieving harmonized port security training in Europe - a critical review of EU legislative frameworks. *Journal of Transportation Security,* vol. 6**,** no. 4, pp. 357-375.

Wengelin, M. (2006). The Swedish port security network – an illusion or a fact? *Journal of Homeland Security and Emergency Management,* vol. 3**,** no. 1, pp. Article 8.

Wengelin, M. (2008) *Is there a Nordic model for societal security and safety?* SAMRISK.

Wengelin, M. (2012) *Service, Regulations, and Ports: An Actor-Network perspective on the social dimension of Service-Dominant Logic.* Lund University.

Whelan, C. (2016). Managing dynamic security networks: Towards the strategic managing of cooperation, coordination and collaboration. *Security Journal,* vol. 30**,** no. 1, pp. 310-327.

Whittle, A. & Spicer, A. (2008). Is Actor Network Theory Critique? *Organization Studies in Higher Education,* vol. 29**,** no. 4, pp. 611-629.

Yanga, Z., Ngb, A. K. Y. & Wang, J. (2013). A new risk quantification approach in port facility security assessment. *Transportation Research,* vol. 59**,** no. 1, pp. 72-90.

Yin, R. (2014) *Case study research: design and methods.* 5th ed. London, UK: SAGE.

APPENDIX I

Survey

Genomgång av regelverk för sjöfarts- och hamnskydd inom den svenska hamnsektorn

- En analys av barriärer för att efterleva de regelverk och riktlinjer som finns för sjöfarts- och hamnskydd på en global, internationell och nationell nivå

* Required

Namnlöst avsnitt

Del A

1. **1. Vilken hamn arbetar du för?**

2. **2. Vilken är din position inom hamnen?**

3. **3. Är hamnen du arbetar för en ISPS- (International Ship and Port Facility Security Code) hamn?** *
   Mark only one oval.
   - ◯ Ja
   - ◯ Nej

4. **4. Är du ansvarig eller inblandad i sjöfarts- och hamnskyddsfrågor för den organisation du arbetar för?** *
   Mark only one oval.
   - ◯ Ja
   - ◯ Nej

5. **5. Hur många ton gods hanterar er hamn på en årlig basis?** *
   Mark only one oval.
   - ◯ Mindre än 10 miljoner
   - ◯ Mellan 10 och 20 miljoner
   - ◯ Mer än 20 miljoner

6. **6. Vilka fartygstyper hanterar er hamn? (vänligen fyll i samtliga överensstämmande alternativ)** *

Check all that apply.

- [ ] Färjor, Kryssning och Ro-Ro
- [ ] Container och Lo-Lo
- [ ] Specialiserade laster (ex högvärdiga skogsprodukter, kyllaster, nya bilar m.m)
- [ ] Bulk och generella laster (ex olja, kemikalier, gas, kol, malm, säd m.m)

Del B.

7. **1. Till vilken grad upplever du/ni att er hamn har möjlighet att efterleva följande regelverk?** *

Mark only one oval per row.

	0 Behöver ej efterfölja	1 Mycket låg grad	2	3	4	5 Mycket hög grad
International Ship and Port Facility Security (ISPS) Code	◯	◯	◯	◯	◯	◯
Europakommissionens Förordningen 725/2004 om ökat sjöfarts- och hamnskydd	◯	◯	◯	◯	◯	◯
Europakommissionens Direktiv 2005/65/EG om ökat hamnskydd	◯	◯	◯	◯	◯	◯
Sveriges Riksdags Lag (2004:487) om sjöfartsskydd	◯	◯	◯	◯	◯	◯
Sveriges Riksdags Lag (2006:1209) om hamnskydd	◯	◯	◯	◯	◯	◯
Sveriges Regerings Förordning (2004:283) om sjöfartsskydd	◯	◯	◯	◯	◯	◯
Sveriges Regerings Förordning (2006:1213) om hamnskydd	◯	◯	◯	◯	◯	◯
Transportstyrelsens Föreskrift (SJÖFS 2004:13) om sjöfartsskydd	◯	◯	◯	◯	◯	◯
Transportstyrelsens Föreskrifter (SJÖFS 2007:1) om hamnskydd	◯	◯	◯	◯	◯	◯

8. **2. Till vilken grad anser du/ni att samarbetet, avseende sjöfarts- och hamnskydd, fungerar mellan er hamn och följande organisationer?** *
Mark only one oval per row.

	1 Mycket låg grad	2	3	4	5 Mycket hög grad
Transportsstyrelsen / Sjöfartsverket					
Tullverket					
Polismyndigheten					
Kustbevakningen					
Privata aktörer (t.ex. vaktbolag)					

9. **3. Till vilken grad upplever du/ni att följande resurser finns tillgängliga för er hamn för att kunna efterfölja samtliga regelverk och riktlinjer kring sjöfarts- och hamnskydd?** *
Mark only one oval per row.

	1 Mycket låg grad	2	3	4	5 Mycket hög grad
Finansiella					
Kunskap					
Personal					
Tid					

10. **4. Till vilken grad anpassar ni ert arbete kring sjöfarts- och hamnskydd, vid hantering av olika fartygstyper och godsslag?** *
Mark only one oval.

	1	2	3	4	5	
Mycket låg grad						Mycket hög grad

11. **5. Till vilken grad upplever du/ni att er organisation förmår att inom organisationen dela och sprida kunskap om sjöfarts- och hamnskydd?** *
Mark only one oval.

	1	2	3	4	5	
Mycket låg grad						Mycket hög grad

Del C.

12. **1. Tycker du/ni att regelverk och riktlinjer för sjöfarts- och hamnskydd borde vara mer lokalt anpassade?** *
Mark only one oval.

- Ja
- Nej

13. **2. Skulle du/ni vilja se en utveckling av nuvarande regelverk och riktlinjer för sjöfarts- och hamnskydd?** *

Mark only one oval.

- ◯ Ja
- ◯ Nej

14. **3. Tycker du/ni att internationella regelverk och riktlinjer för sjöfarts- och hamnskydd borde innehålla tydligare metoder och verktyg för implementering?** *

Mark only one oval.

- ◯ Ja
- ◯ Nej

15. **4. Tycker du/ni att regelverk och riktlinjer för sjöfarts- och hamnskydd borde vara mer anpassade efter de fartygstyper och godsslag en hamn hanterar?** *

Mark only one oval.

- ◯ Ja
- ◯ Nej

Del D.

16. **1. Vilka hinder upplever du/ni (om några) att ni har för att följa lagar och förordningar inom sjöfarts- och hamnskydd?** *

APPENDIX II

Intervjuguide - sakkunniga

Informera om:

- Anonymitet
- Sammanställning av intervju till intervjuperson efteråt, översättning till engelska
- Är det ok att spela in intervjun?
- Respondenten får hoppa över frågor eller avsluta intervjun när denne så önskar

Bakgrundsinformation

- Vad är din bakgrund?
- (Om det behövs) Beskriv din bakgrund inom sjöfarts- och hamnskydd närmare.

- Vi beskriver vår studie, vilken datainsamling vi har gjort hittills och varför personen tillfrågats att delta i studien.

- Intervjun är uppdelad i tre delar samt en avslutande sammanfattning, där vi redogör vad vår enkät har för resultat. Därefter vill vi ställa lite frågor kring resultaten och höra din uppfattning samt dina tankar och funderingar.

Regelverk och riktlinjer

Enligt vår undersökning, har resultatet visat på en trend där svenska hamnar upplever att det är svårare att efterleva regelverk på en nationell nivå i jämförelse med de regelverk som finns på en internationell och global nivå (se figur 2 och 3).

1. Vad tror du kan vara den bidragande orsaken till att hamnarna upplever att det är svårare att efterfölja de nationella regelverken jämfört med de internationella och globala regelverken?
2. Resultatet visar också på att hamnar som hanterar passagerare, generellt sett upplever en högre grad av efterlevnad än övriga hamnar. Vad tror du kan vara orsaken till detta (figur 4)?

Enligt vår undersökning, visar resultatet på att de svenska hamnarnas upplevda möjlighet att efterfölja regelverk för sjöfarts- och hamnskydd i stor utsträckning speglar resultatet från tillgängliga resurser inom organisationen för efterlevnad av regelverk (se figur 10). (Förklara hur figur 10 tagits fram).

3. Vad anser du om det samband som identifieras mellan den individuella hamnens resurstillgänglighet och deras upplevda förmåga att efterfölja regelverken (figur 10)?
    - Hur anser du att resurstillgänglighet (personal, tid, finansiellt och kunskap) kan bidra som faktor till hamnars möjlighet att efterleva regelverk för sjöfart- och hamnskydd?

- Är det mycket resursers som möjliggör efterlevnad eller är det god efterlevnad som gör att resurser anses finnas i större mängd?

Enligt vår studie anser större hamnar att de har tillgång till mer resurser än små hamnar figur 7, och passagerarhamnar anser att de har större tillgång till resurser än hamnar som ej är passagerahamnar figur 8.

Hälften av de tillfrågade hamnarna har uttryckt ett behov av att anpassa regelverken efter de fartyg och godsslag hamnen hanterar (se figur 16). Framförallt visar resultatet på att mindre hamnar upplever ett större behov av att anpassa regelverken (se figur 17).

4. Vad är din uppfattning om detta? Tror du att det är genomförbart? På vilka nivåer, lagmässigt, ska/kan detta genomföras?
    - Vem är enligt din uppfattning ansvarig, den individuella hamnen eller lagstiftande organ, för hamnskyddet och dess anpassning efter fartyg och godsslag?
5. Vad tror du är den bakomliggande anledningen till att mindre hamnar upplever ett större behov?

Passagerarhamnar, enligt undersökningen, anpassar sitt skyddsarbete mer än övriga hamnar (figur 9)

Enligt vår enkät, har en majoritet (60%) av de svenska hamnarna som deltagit i undersökningen, uttryckt ett behov för en utveckling av existerande regelverk och riktlinjer kring sjöfarts- och hamnskydd (se figur 13).

6. Vad är din uppfattning om detta? Tror du att det är genomförbart? På vilka nivåer, lagmässigt, ska/kan detta genomföras? Åt vilket håll bör regelverken utvecklas?

På en internationell nivå – där 67% av de svarande anser att det finnas behov av tydligare verktyg och metoder för implementering av regelverken (se figur 14). Samtliga mindre hamnar anser att det behövs tydligare verktyg och metoder för implementering (figur 15). Dessutom anser mindre hamnar att det finns ett större behov för lokal anpassning av regelverk för sjöfarts- och hamnskydd (figur 12).

7. Vad är, enligt din uppfattning, de bakomliggande orsakerna kring dessa två behov?
8. Varför tror du hamnarna riktar behovet av tydligare verktyg och metoder till de internationella regelverken och inte till de svenska regelverken?
9. Borde man anpassa regelverken för lokala nivåer eller borde man införa tydligare verktyg och metoder på en globalnivå? Enligt litteraturundersökningen är forskare delade på denna punkt, men ingen har identifierats som anser att man kan genomföra båda, utan förespråkar det ena eller andra. Hur ser du på detta?

Skyddsnätverk

Tidigare studier som gjorts kring området för sjöfarts- och hamnskydd, visar på att bristfälligheter i ett skyddsnätverk orsakas/uppstår bl.a. i samband med intressekonflikter mellan de olika aktörerna, bristande insikt kring ansvarsområden för de involverade aktörerna samt bristfälligt samarbete parterna mellan. Enligt den enkätundersökning som gjorts, har ett flertal svenska hamnar svarat att samarbetet med olika myndigheter som ansvarar för/ är involverade i arbetet kring sjöfarts- och hamnskydd, till viss del är bristfällig (figur 19).

10. Vad anser du kan vara de bakomliggande problem som ligger till grund för brister i samarbetet mellan de aktörer som utgör sambandspunkt för sjöfarts- och hamnskyddsfrågor i Sverige?
    - Hur ställer du dig till resonemanget att intressekonflikter och dålig insikt om ansvarområde bland aktörerna, kan vara en orsak till bristfälligheter samarbetet?
    - Enligt din uppfattning, vilka fördelar/nackdelar finns det med att ha ett nätverk för hamnskydd?
    - Hur skulle detta samarbete kunna förbättras för att på så sätt stärka sjöfarts- och hamnskyddet i svenska hamnar?
    - Enligt din uppfattning, hur skulle ett idealt skyddsnätverk för hamnskydd se ut? Vilka aktörer skulle vara involverade?

Skyddskultur

Från tidigare studier som gjorts kring området sjöfarts- och hamnskydd, har det framkommit att bristfälligt ledarskap och organisering av skyddskultur inom organisationer, bland annat pga. otillräcklig utbildning och träning för personal, leder till bristande skyddstänk bland de anställda. Detta i sin tur ökar riskbilden för skyddsrelaterade hot som organisationen kan utsättas för.

11. Enligt din uppfattning, hur avgörande är det att en hamnorganisation har en effektiv och välfungerande skyddskultur?
12. Hur ska man som hamnorganisation möjliggöra för en effektiv skyddskultur? Vilka kan enligt din mening vara de bidragande faktorerna som hämnar en effektiv och välfungerande skyddskultur?

Sammanfattning och uppföljning

13. Vilka barriärer anser du vara de största för svenska hamnar för att efterleva sjöfarts- och hamnskydd?

14. Är det något du vill tillägga eller förtydliga?

APPENDIX III

Intervjuguide - Transportstyrelsen

Informera om:

- Är det ok att spela in intervjun?
- Sammanställning av intervju till intervjuperson efteråt – den kommer översättas till engelska
- Respondenten får hoppa över frågor eller avsluta intervjun när denne så önskar
- Du som person är anonym.
- Vi vill ha tillåtelse att använda det du säger som kommentarer från TS?

Bakgrundsinformation

- Vi beskriver vår studie, vilken datainsamling vi har gjort hittills och varför vi bett TS delta och kommentera.

Frågeställning

I vår enkätundersökning frågade vi de svenska hamnarna hur de upplever att samarbetet fungerar med de övriga aktörerna som utgör Skyddsnätverk för sjöfarts- och hamnskydd i Sverige (Skyddsnätverk: Transportstyrelsen, Polisen, Tullen, Kustbevakningen och Privata aktörer). Resultatet, som presenteras i figur 18 respektive figur 19, visar på de Svenska hamnarnas upplevda samarbete med de olika aktörerna.

1. Hur resonerar ni kring det resultat som presenteras i de båda figurerna?

2. Kan resultatet som presenteras, indikera på att samarbetet mellan hamnarna och övriga aktörer i skyddsnätverket till viss mån är bristfälligt?
    - Och vilka eventuella konsekvenser kan detta ha på ett effektivt och välfungerande hamnskydd i Sverige?

3. Hur skulle ett bättre samarbete mellan er och hamnarna se ut om ni fick bestämma?
    - Vilka faktorer anser ni är bidragande till att det inte ser ut så idag?

I vår studie indikerar resultaten på att kunskap och informationsspridning är väsentliga faktorer för att skapa ett bra och välfungerande skydd.

4. Hur arbetar ni idag med att sprida kunskap och information till hamnar gällande skyddsfrågor och efterlevnad av regelverken?

- Kan denna kunskaps- och informationsspridning förbättras, i så fall hur?

5. Delar ni ansvaret att sprida kunskap och information med andra aktörer?

6. Vilka för- och nackdelar anser ni att det finns med transparens gällande skydd?
   - Vilka fördelar kan mer information leda till?
   - Vilka nackdelar kan mer information leda till?

7. Hur många inspektörer har ni som kontrollerar efterlevnad för hamnarna i Sverige?
   - Arbetar de heltid med enbart inspektion? Hur ser deras arbetsroll ut?

8. Har ni personal som besöker samtliga hamnar som inte gör besök för att utföra kontroller, utan vars uppgift är att sprida kunskap och förmedla vart hamnarna kan vända sig för att få hjälp med efterlevnad av regelverken?
   - Om ja, hur ser den ut och hur ofta sker detta, får samtliga hamnar besök eller måste hamnen själv ta kontakt med er för att få till en träff?
   - Om nej, varför inte? Skulle det finnas några fördelar med ett sådant koncept anser ni, vilka?

9. Skiljer det sig hur ofta och vilken typ av kontakt ni har med hamnar beroende på hamnarnas storlek, godskapacitet och godsslag?
   - Finns det hamnar som får mer assistans av er än andra hamnar?
   - Om ja, vilken typ av hamnar är det? Varför blir de prioriterade?
   - Om nej, vilka är för- och nackdelarna med att hamnar har samma prioritet oavsett storlek och godsslag?

Enligt vår enkät vill mindre hamnar att de ska finnas tydligare metoder och verktyg för att implementera regelverken (figur 14 och 15).

10. Skulle tydligare metoder och verktyg för implementering och efterlevnad av regelverken, ha några konsekvenser och vilka skulle det vara i så fall?

I nuläget indikerar vårt resultat på att det finns eventuella intressekonflikter mellan de aktörer som utgör skyddsnätverk för sjöfarts- och hamnskydd i Sverige. T.ex. att hamnar kan prioritera sina kommersiella intressen framför att säkerställa ett effektivt och välfungerande hamnskydd. Samtidigt som Transportstyrelsen kan ha intresse av att upprätthålla hamnskydd (genom strikta skyddsåtgärder lagmässigt) som ska efterlevas och därmed kräver extra resurser från hamnarnas sida.

11. Upplever ni att det finns eventuella intressekonflikter mellan de aktörer som utgör skyddsnätverk för sjöfarts- och hamnskydd i Sverige? (Skyddsnätverk: Transportstyrelsen, Polisen, Tullen, Kustbevakningen, Privata aktörer och Hamnar)
    - Om ja, vilka intressekonflikter anser ni vara de mest framträdande i nätverket som i sin tur påverkar ett effektivt och välfungerande samarbete inom nätverket?
    - Hur kan man arbeta inom nätverket för att minska intressekonflikternas inverkan på nätverket i så stor utsträckning som möjligt?
    - Hur kan intressekonflikter arbetas bort eller är de inbyggda i det systemet som idag finns och omöjliga att bli av med om man behåller nuvarande system?

12. Upplever ni att ansvarsfördelningen inom nätverket är tydligt fördelad och att samtliga aktörer uppfyller sina respektive funktioner i nätverket eller finns det brister?
    - Om det finns brister, vad bör göras för att samordna detta bättre?

---

13. Har ni några övriga kommentarer på intervjun eller på våra enkätresultat?

---

14. Vilka barriärer anser ni vara de största för svenska hamnar att efterleva regelverken om sjöfarts- och hamnskydd?