10-31-2021

Maritime cybersecurity: comparing practices between developing countries : the case study of Kenya and Spain

Bibian Turyahumura

WORLD MARITIME UNIVERSITY
Malmö, Sweden

Maritime cybersecurity - comparing practices between developing countries and developed countries - the case study of Kenya and Spain.

By

BIBIAN TURYAHUMURA
Republic of Uganda

A dissertation draft submitted to the World Maritime University
in partial
fulfilment of the requirements for the reward of the degree of

MASTER OF SCIENCE
in
MARITIME AFFAIRS

(MARITIME ENERGY MANAGEMENT)

2021

DECLARATION

This is to certify that all the information in this dissertation that is not my own work has been cited/referenced, and that no material is included for which a degree has previously been conferred on me. The contents of this dissertation reflect my personal views, and are not necessarily endorsed by the University.

Signature:

Date: September 17, 2021

Supervised by: Dr. Fabio Ballini

Supervisor's affiliation: Professor - Maritime Offshore Facilities
Maritime Energy Management Specialization
WORLD MARITIME UNIVERSITY

ACKNOWLEDGEMENTS

This study has been a tumultuous one for me, starting with remote learning in the face of COVID-19, going through challenges collecting information in light of lockdowns and travel restrictions across Europe and Africa. Nonetheless, God has been faithful and has seen me through this all up to this point.

I would like to acknowledge and thank my Sponsor Sasakawa Foundation fully funded my Masters studies at World Maritime University, without him my studies would have never been there, my greatest appreciation to my specialization professors to mention especially my research supervisor – Professor Fabio Ballini, Monica Canepa for their great insights and guidance during this process of research. I would also like to thank my study colleagues, my family especially my mother – Peace Mugabwire for being there for me and providing moral support during this year of absence from her.

Thank you to my employer, the Ministry of Works and Transport in Uganda, staff of the ports of Valencia and Mombasa that were very helpful in providing data for this research without which I would not have successfully completed this.

All glory and honour go to God.

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

ABSTRACT

Title of Dissertation: **Maritime cybersecurity - comparing practices between developing countries and developed countries - the case study of Kenya and Spain.**

Degree: **Master of Science**

The rapid technological change in the maritime industry requires a consciousness of the impacts and scope of cyber threats and cybersecurity risks. This study investigated the relationship between maritime cybersecurity risks and threat mitigation measures, comparing developed – Spain, and developing – Kenya – IMO member states. Using a case study approach with a qualitative research design and focusing on cybersecurity in port operations and shipping, the study results showed that the cybersecurity strategy implementation in Europe far outpaces that of Africa. The study established that the models of cybersecurity measures pursued by European and African ports faced an outstanding risk accrued to the slow adaptation of cybersecurity strategy, implementation to the rapid change in technology and innovation such that these strategies become obsolete before optimal use. This is in addition to infrastructure challenges, talent for cybersecurity, technology, strategy, governance, crime/fraud, reputation, and regulation, among others.

The study demonstrated the need for cybersecurity to be incorporated into both the European and African maritime security apparatuses and frameworks by institutionalizing the responses of member states in relation to these types of security risks including raising awareness around the vulnerability and cyber threats concerning the maritime sphere.

The research concludes by stating that, greater effort should be focused towards making sure maritime cybersecurity keeps up the with the changes in technology. Given the pervasiveness of non-African indication on maritime cybersecurity incidents, increased Africa-specific knowledge and research is required.

KEY WORDS: Maritime Cybersecurity, Maritime cyber policy, Port Digitalization, Port energy management, Maritime cyber systems, Information security.

TABLE OF CONTENTS

DECLARATION i

ACKNOWLEDGEMENTS ii

ABSTRACT iii

TABLE OF CONTENTS iv

LIST OF TABLES vi

LIST OF FIGURES vii

LIST OF ABBREVIATIONS viii

1.1. Introduction and background 1
1.2. Problem Statement 3
1.3. Purpose of the study 4
1.4. Objectives of the study 4
1.5. Research Questions 4
1.6. Limitations of the Study 5
1.7 Research Outline 6

CHAPTER 2: LITERATURE REVIEW 8
2.1. An analysis of port digitalization 8
2.2. Taxonomy of Maritime Cyber Threat 9
2.3. Cybersecurity and the Maritime Supply Chain 12
2.4. Maritime Cyber Policy and Regulations 13
3.1. Introduction 17
3.2. Research Scope and Activities 18
3.3. Data Collection and Analysis 19
3.4. Description of Colaizzi's Framework for Qualitative Data Analysis 20
3.5. Description of the McKinsey 7S Model 22
3.6. The PESTEL Framework 24
3.7. Description of the SWOT Analysis Framework 26

CHAPTER 4. MARITIME CYBERSECURITY IMPLEMENTATION IN DEVELOPED AND DEVELOPING COUNTRIES 28
4.1. International Maritime Cybersecurity Perspective 28
4.2. Maritime Cybersecurity in Europe Vs. Africa 29
4.2.1. Spanish (EU) Maritime Cybersecurity Policy Overview 29
4.2.2. African Maritime Cybersecurity Policy Overview 30
4.3. Implementation of Maritime cybersecurity: Best Practices 31
4.3.1. Port of Mombasa (Kenya) 32
4.3.2. Port of Valencia (Spain) 32

CHAPTER 5. CASE STUDY OF KENYA AND SPAIN 34
5.1. Cybersecurity Implementation at Mombasa Port 34
5.1.1. Overview of Mombasa Port 34
5.1.2. Cyber Risk and Threat Management at Mombasa Port 35

5.1.3. SWOT analysis for cybersecurity strategy implementation at Mombasa Port 40
5.1.4. GAP Analysis: McKinsey 7-S Framework and PESTEL. 43
5.2. Cybersecurity Implementation at Valencia Port **49**
5.2.1. Overview of Valencia Port 49
5.2.2. Cyber Risk and Threat Management at the Port of Valencia 50
5.2.3. SWOT analysis for cybersecurity strategy implementation at Port of Valencia Port 53
5.2.4. GAP Analysis: McKinsey 7-S Framework and PESTEL 57
5.3. Maritime Cybersecurity Implementation Metrics assessment in developed (Europe) and developing (Africa) Countries **63**
CHAPTER 6. CONCLUSION AND RECOMENDATION **66**
6.1. Conclusion **66**
6.2. Summary of Findings **68**
6.3. Recommendation **69**
REFERENCES **73**

LIST OF TABLES

Table 3.1: Colaizzi's Framework for qualitative data analysis (Morrow, Rodriguez, & King, 2015) 21
Table 5.2: Mombasa Port Cybersecurity Strategy Analysis using the McKinsey 7s Framework 43
Table 5.3: Kenya/Mombasa Port Analysis using the PESTEL Framework 46
Table 5.4: SWOT analysis for cybersecurity strategy implementation at Valencia Port 54
Table 5.5: Spanish/Port of Valencia Cybersecurity Strategy Analysis using the McKinsey 7s Framework 57
Table 5.6: Port of Valencia Analysis using the PESTEL Framework 60
Table 5.7: Cybersecurity threat and risk mitigation measures at the two ports 63

LIST OF FIGURES

Figure 1.1: Flowchart showing the research approach (Source: Author) 7

Figure 3.1: Research Activities 18

Figure 3.2: Framework concept for systematic literature analysis (Adapted from: Vom Brocke et al., 2009) 20

Figure 3.3: The McKinsey 7S Model 23

Figure 3.4: The PESTEL Framework 25

Figure 3.5: The SWOT Analysis Framework 26

Figure 5.1: The overview map of Mombasa Port, Africa ports. 35

Figure 5.2: Map of Port of Valencia. Maps Valencia. (2021, 08). 50

Figure 5.3: Main Services, Activities and Infrastructure at Port of Valencia, Port du Valencia (2019) 51

LIST OF ABBREVIATIONS

AIF	Artificial Intelligence Fuzzing
AIS	Automatic Identification System
BIMCO	The Baltic and International Maritime Council
CPS	Cyber-Physical Systems
ENISA	The European Union Agency for Network and Information Security
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IIoT	Industrial Internet-of-Things
IMO	International Maritime Organization
ISM	The International Safety Management Code
ISPS	The International Ship and Port Facility Security
ISS	The Institute for Security Studies
IT	Information Technology
JIT	Just In Time
ML	Machine Learning
NC3	The National Cyber Command Center
OT	Operation Technology
PFSA	Port Facility Security Assessment
SOLAS	International Convention for the Safety of Life at Sea
USB	Universal Serial Bus

CHAPTER 1. INTRODUCTION AND BACKGROUND

1.1. Introduction and background

Globalization has manifested in fast-paced innovations and developments, especially in the area of technology and cyber-systems (Frøystad et al., 2017).This has affected all sectors including the maritime sector. The global maritime sector has over the past decade seen the proliferation of the use of cyber systems (International Maritime Organization, 2017) for example maritime control systems (Lag et al., 2015), and maritime navigation systems (Lloyd's Register, 2017), bridge systems, communication systems, machinery control and propulsion systems, access control systems, cargo handling and management systems etc. These systems have helped improve operational efficiency, marine human resources productivity, and have helped optimize performance in the maritime sector. The advent of the Internet of Things (IoT) where devices interact with each other with little or no autonomy has led to increasing interdependence of one system to another.

However, the interdependence on these systems and their increasingly inextricable interactions poses a threat in the likelihood of any cyberattacks (World Economic Forum, 2020). The development of cyber systems has met serious security threats globally (Viano, 2017) and the maritime sector has not been spared these threats(Robert Lemos, 2019). The threats manifest on ships in areas such as ICT systems on ships that are connected to the internet, communication systems, geo-location systems and at the ports in areas such as Port-office IT Systems, AIS (Automatic Identification Systems) gateways, Vessels Traffic Services (VTS), and Industrial Control Systems (ICS) (MARSH, 2014). Time has shown that these threats have had grave consequences for ships, their personnel, ports, states and their economies(Rose et al., 2017).

Efforts have been made at global, continental, regional and state level to prepare for and mitigate threats to maritime cyber systems through the introduction of cybersecurity guidelines (International Maritime Organization, 2017), the creation of

maritime cybersecurity bodies or organizations like the Baltic and International Maritime Council (BIMCO) (Baltic and International Maritime Council, 2020) or event state-level maritime cybersecurity laws (Ringsberg & Cole 2020) . The pace of state regulation and management of these cyber systems has not matched the rate at which these systems are being developed and adopted (Tam & Jones, 2018) as well as the speed at which malicious attacks are growing (Hellenic Shipping News, 2020) more so, when looking at third world and developing nations.

Research (Hellenic Shipping News, 2020) shows that the threat of cybersecurity is not about to reduce. While many developed states for example European states like Sweden (The Swedish Club, 2021) have instituted measures against maritime cybersecurity threats, in line with IMO's maritime cybersecurity guidelines (International Maritime Organisation, 2017) and European Maritime Cybersecurity standards (European Union Agency for Cybersecurity, (ENISA), 2020), poor and developing states in sub-Saharan Africa for example Kenya, Tanzania and Uganda have a long way to go (Reva, 2020). Research has shown an increasing interest in helping build cybersecurity capability through the use of cybersecurity maturity models(Baltic and International Maritime Council, 2020) but this has largely remained a preserve of developed states.

Cyber Systems and Port Energy Management

According to (UNCTAD, 2019), the digitalization of oceanic transport can be categorized into phases. In the first phase, the focus of this study, smart logistics operations are known to have now to a noteworthy fall in expenditures on inventory assets and at the same time, more money is being spent on reliable, fast and just-in-time conveyances. More and more port terminal processes and ship navigation are becoming automated – even in developing countries. A number of recent initiatives are gauging the optimization chances that concurrently come with these novel technologies. Optimization of port-call is, for example, optimizing vessel routes and speeds thereby reducing waiting times in ports and subsequently carbon-dioxide emissions (Port of Rotterdam, 2018). The authorities of ports and operators of

terminals have galvanized forces to optimize port and intermodal connections (Global Institute of Logistics., 2017).

According to (Container x-change, 2020), ports utilize IoT and big data for resourceful decision making and management of logistics, ports can also make use of big data and predictive analysis to schedule the vessel's arrival/departure for just-in-time (JIT) arrival thereby improving the overall efficiency of ports. If this is done, it would help in congestion management on the ports by circumventing ship idling and as well as preventing them from using up excess power on ports. It would also additionally save ship fuel by way of controlled ship speed, and at the same time cutting down emissions. Additionally, it should be noted that adopting automation, smart technology and IoT would go a long way in helping to reduce the carbon footprint massively through better asset management and port operations.

1.2. Problem Statement

The advent, use and adoption of cyber technology/cyber systems in the maritime sector, while improving operational and transactional efficiency (Lloyd's Register, 2017) has not been in synch with both the pace of change in this technology as with other sectors (Lehto, 2020), the rate of growth of malicious attacks (Androjna et al., 2020) as well as IMO-member states' creation of regulations to stem the risks accrued to the adoption of this cyber technology for day-to-day work (Hopcraft & Martin, 2018) . This aside, the rate of regulation differs greatly between developed states and undeveloped states and little attention has been paid to supporting developing states through a maritime cybersecurity maturity journey. If the adoption and regulation rate continue in a "business-as-usual" style, the maritime sector faces potential catastrophic cybersecurity risks/threats (Hellenic Shipping News, 2020). Further to that, the disparity in implementation of cybersecurity guidelines/measures across IMO member-states leaves the maritime cybersecurity ecosystem open to cyber threats.

1.3. Purpose of the study

The purpose of the study is to investigate the relationship between maritime cybersecurity risks and threat mitigation measures across developed and developing IMO member states.

1.4. Objectives of the study

1. To establish the difference between the developed countries (for example, Spain) and developing countries (for example, Kenya) with respect to:
    a. maritime cybersecurity threats
    b. Maritime cybersecurity threat mitigation measures
    c. Maritime cybersecurity maturity
2. To examine the difference between developed countries (Spain) and developing countries (Kenya) with regard to implementation of IMO's maritime cybersecurity guidelines.
3. To identify and recommend state-level maritime cybersecurity initiatives that would help developing countries improve their maritime cybersecurity maturity.

1.5. Research Questions

1. How can the difference between developed countries (Spain) and developing countries (Kenya) with respect to maritime cybersecurity threats, mitigation measures, and maturity and implementation in relation to IMO's maritime cybersecurity guidelines be examined and established?
2. How can the challenges and barriers to maritime cybersecurity implementation in developed countries (Spain) and developing countries (Kenya) be examined?
3. How can state-level maritime cybersecurity initiatives that would help developing countries improve their maritime cybersecurity maturity be identified and recommended?
4.

1.6. Limitations of the Study

Some respondents did not feel free to share all the information that was necessary for the study. To mitigate this limitation, the researcher explained all the study objectives and assured the respondents that information provided would be dealt with confidentially and would only be used for study purposes.

Setting and managing the interview appointments was a problem which led to delay in the schedule of the research. This was alleviated by use of a data collection guide, specifically, interview guide.

This research used only two (2) ports as case study. However, this is a rather small number to explain the entire population of ports. To enhance the robustness of the results, one should expand this sample. With a larger sample, the results found are more representative for the entire population of ports.

The study relied majorly on port employees and not much on other parties that may impact and influence cybersecurity implementation in ports such as MartitmeTech, and BigTech etc. Further study could be carried out to cover these parties.

Reliance on reports that may convey biased portrait: Some documentary sources on which this dissertation relied for data were produced by the case organizations. One might consider that they convey a biased portrait of cybersecurity implementation in the organization. However, the documents used as data sources are not entirely reports on cybersecurity, but also internal documents aimed at the organization themselves that provide policy and operational guidance of how the port implements cybersecurity.

Finally, due to the short timescale of the research in regard with and comparison to the research area, the researcher was not able to study exhaustively further in the field. The researcher therefore chose to limit the scope of the study by using two case organizations only as target population.

1.7 Research Outline

This dissertation consists of six chapters organized as follows; Chapter one introduces the research topic, giving the background relating to cybersecurity implementation in the maritime industry, the problem statement, the research objectives and questions, and the limitation of the research. In chapter two, existing literature on maritime cybersecurity is reviewed, analyzing its implementation in ports including the policy and regulation. Chapter three explains the methods used to collect and analyze the data, describing the framework used. Chapter four looks at the cybersecurity implementation practices in developing (Kenya) and developed countries (Spain), including policies, frameworks and best practices in ports from the international, regional and national perspectives. Chapter five covers the case study of Mombasa port in Kenya and Valencia port in Spain with respect to maritime cybersecurity implementation practices. The findings of the research are consequently presented under chapter five, highlighting the cybersecurity implementation practices of the two ports with respect to international standards especially the IMO guidelines. The conclusion and recommendations to beneficiaries follow in chapter six. The approach used to conduct the research is illustrated in Figure 1.1.

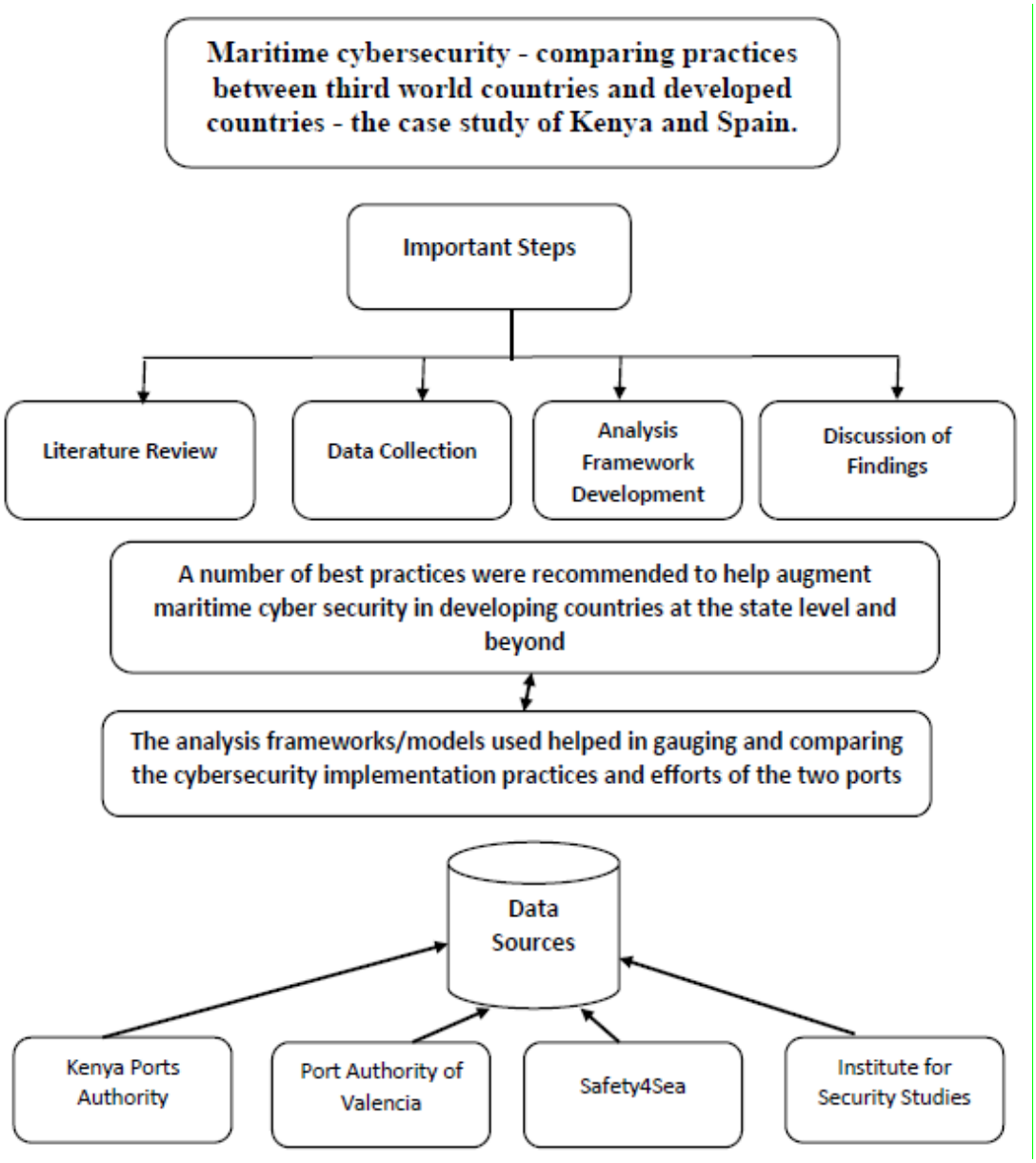

Figure 1.1: Flowchart showing the research approach (Source: Author)

The approach taken meant to address the research questions in order to achieve the stated objectives of the study. A discussion of the finding was made, and recommendations on cybersecurity implementation at Mombasa port and also port of Valencia was discussed to help port management and stakeholders make smart decisions during investments and implementation.

CHAPTER 2: LITERATURE REVIEW

2.1. An analysis of port digitalization

Digitalization holds extraordinary possibilities for improving the effectiveness, adaptability and agility of maritime transport chains. It hence builds the capability of ports to face globalization and urbanization challenges. Digital and electronic solutions can help improve the effectiveness of harbours their respective transport chains, expanding them and disentangling their complex formations and decreasing energy utilization. Within the worldwide sea-environment economy, automation and computerization of seaports operations provide the impetus to promote effectiveness and security along the sea transport value chain. Ports are now able to create and utilize contemporary commerce models (Fraunhofer, 2021).

Industry /business 4.0 – associated with a fourth industrial revolution is manifested in the permeation of individual and social lives by inter-connected and novel technologies, business processes and ideas like cloud computing, big data, self-administration by machines and mobile computing, automated and self-navigation modules and services. Industry/ Business 4.0 is therefore becoming a critical requirement for economic growth (Broy,2010), Industry 4.0 leverages data, Information and communication technologies (ICT) (Keller, M., Pütz, S., & Siml, J, 2012). Like other industries, the maritime sector interactively leverages computing for example, working with digitized items through of storage, networking, programmability, sensors or capability which can permit a rise within the potency of operations of ports and ships (Jahn et al., 2011). According to (Berg & Hauer, 2015), the shipping industry utilizes weather data, log files from Automatic Identification Systems (AIS), fuel-sampling data, and big data to analyze and subsequently compare business and operational performance with alternative firms. The maritime industry therefore leverages transport processes that are multimodal that are networked and synchronized across the maritime transport value chain by independent actors thereby optimizing traffic and product movements (Berg & Hauer, 2015).

Digital transformation and the utilization of big data utilization enable the optimization of fleet controls, in such a way that the environmental protection is improved and costs

reduced. It is possible to optimize the control and flow of traffic by using the operating data of ships, subsequently avoiding crucial circumstances and therefore decreasing the likelihood of accidents. Ship data, for example, aggregated, cargo, weather and machine data, are transferred in real time to inland/on-port management in real time thereby enabling a two-way interaction between the aggregated data and the ship's management (Arndt, 2016). The downside to this digital revolution include ethics issues like privacy, reduced self-sufficiency and increased reliance of customers on ICT firms, all of which represent moral and ethical challenges from an economic, information al and technological perspective (Bendel, 2015).

To this effect, the success of technological and digital transformation of in the maritime supply-chain is contingent on the inclusion of data security and data protection the port management implementation strategy. Operation and management of digital applications and technologies doesn't solely need competent users well versed with digital platforms or innovations, but rather guaranteed systems security, internal infrastructure and operating systems' protection from cyberattacks for maritime firms (Schweer & Sahl, 2016). It should therefore be noted that the maritime supply chain digitalization and the subsequent effects associated to it are a gigantic field that require structuring and prioritization scientifically.

2.2. Taxonomy of Maritime Cyber Threat

It should be pointed out that there is a lengthy account of an attempt to build consciousness in the maritime industry's operations to cyber threats and their impacts albeit from an exclusively physical perspective. Recently, the evolution of the maritime industry has driven it towards an over reliance on technology. This literature gives a comprehensive view of contemporary cyber security in the maritime industry, including ultra-modern and cyber-attacks threats. There has been an upsurge in the volume of cyber threats (Burt, 2020), (The Maritime Executive, 2020), and on the other hand, the world maritime fleet is continuously growing for example 18.2% between 2015 and 2020 (Infomaritime, 2021) and are constantly becoming more and more dependent technologically. (Burt, 2020) for example argues that Internet of Things (IoT) threats commonly associated with the maritime industry are rapidly and

increasingly snowballing and evolving. The beginning of 2020 saw an estimated 30% upsurge in general volume of attack in comparison with the 2019's second half year. This summarizes the seriousness of the issue.

Cybersecurity threats and challenges in the maritime industry fall under three key themes (The Computer Society, 2020).

I. *Distortion:* This is the use of robots and bots to spread of deception thereby compromising of belief in authenticity when judging data.
II. *Disruption:* Over-dependence on delicate networks increases the likelihood and hazard of planned network blackouts thereby compromising trade operations. For example, ransomware can be used by cyber criminals to capture the IoT.
III. *Deterioration:* quick pushes in savvy advances as well as clashing requests carried out by states aimed at advancing national and transnational security shall affect an enterprises' ability to govern data.

The maritime industry should therefore stay ahead in the following cyber threats facing the industry as argued by (The Computer Society, 2020) and (Kimberly et al., 2016).
Social Engineering Attacks: Social engineering assaults such as phishing has for a long time been utilized by aggressors to trap casualties into surrendering delicate data like login subtle elements and credit card data. Despite the attempts by organizations to improve e-mail security in detecting and blocking phishing assaults, cybercriminals are concurrently improving phishing packs that help breach these security barriers and allow for extortion of ransoms.

Out of Date Software: Software on sea vessels tends to be obsolete owing to; First, the construction of massive ships is costly and time-consuming and most ships were built prior to the emergence cyber security as a major concern. Besides, it is not exceptional for unused computer programs to be incongruent with more seasoned equipment. Hence, outdated programs are frequently kept in utilization.

Vulnerability of Systems: Port systems or ships risk being compromised in an attempt to seize cargo. For example, the ECDIS framework that shows computerized naval

charts is open to compromise (Dyryavyy, 2015) by altering records and embedding content that is malicious.

Cyber Hijacks: Cyber-attacks on different on-board ship or vessel systems or structures may give aggressors control of these targets with a likelihood diverse consequences. For example, posting false information, scrambling key records or framework components and obstructions. The frequent incidence of ransomware in conventional computing and mobile devices is only a step away from being acclimatized to the oceanic space.

AI-enhanced Cyber threats: The disruption of AI and Machine Learning (ML) has permeated each and every industry. AI is being embraced in the maritime industry due to its capacity to support critical decision-making in the administration of the supply chain, marketing, security, manufacturing and other areas. The AI capabilities utilized to recognize and halt cyberattacks is now being utilized to transmit contemporary cyberattacks within computer programs. AI fuzzing (AIF) and Machine Learning (ML) harming are all set to be the following enormous cybersecurity dangers in the maritime industry.

Profit and Cost Axis: Profit-driven malware are getting to be simpler and cheaper to make. Instruments for malware improvement and misuse units are common instruments for aggressors, so that naiveté programmers can cause noteworthy harm. Besides, the low cost of tools required to hack maritime systems has made it easier for cyber criminals given that the systems they attack are mostly obsolete and rudimentary in comparison with other targets.

This study will investigate the relationship between maritime cybersecurity risks and threat mitigation measures across developed and developing IMO member states with the case study being the port of Valencia in Spain and Mombasa in Kenya. The study will cover both port authorities, ship proprietors, nation governments and other stakeholders and will assess the maritime cybersecurity implementation practices of the two countries and discuss the implementation scenarios of maritime technology and cybersecurity for additional benefits to be realized. These are explained under chapter six of this dissertation.

2.3. Cybersecurity and the Maritime Supply Chain

Innovations in Technology have remodelled the globe by altering the landscape of personal communication and expediting the growth of mobile commerce and telework as examples and the commercial landscape has additionally been altered as a result of numerous supporting technologies that are connected to Industry 4.0 as argued by (Culot et al., 2020), Industry 4.0 originated in 2011 from a German technology project. The term refers to the increase in digitalization of processes of industrial activities as argued by (BMBF, 2018).One outstanding technology of Industry 4.0 is IoT, which according to (Li, S. et al., 2015) involves a human-less connection and interaction of various uniquely identified devices. With the term being applied in a business context including maritime, supply chain, and manufacturing, among others, it has taken up the name Industrial Internet of Things (IIOT). (Acharjya et al., 2017) define IIOT as "a network paradigm that consists of physical elements, platforms and software to communicate and share data between them in (a) smart manner". Another related theory, the Cyber-Physical Systems (CPS) defines IIOT as "a next-generation network connected collection of loosely coupled distributed cyber systems and physical systems monitored/controlled by user defined semantic laws, where cyber systems refer to the collections of control logic and sensor units, and physical systems refer to the collections of actuator units". (Ying Tan et al., 2008) and (Greer et al., 2019) argue that CPS and IIoT are essentially hybrid systems that include logical and physical constituents. They state that this system setup raises potential challenges from the cybersecurity viewpoint in the maritime industry.

The maritime logistics sector has drone and robot technologies that are being espoused to expedite movement, distribution and storage of goods and enhance customer service and order fulfilment (Azadeh et al., 2019) ; (Agatz et al., 2018). The key challenge is to manage the integrity of data to have adequate quality assurance of the supply chain and logistics services in the maritime sector and this disquiet can be easily addressed through the implementation of block chain technologies side by side with platforms for Industry 4.0. (Li & Zhou, 2020) argue that block chain assimilates the openness of the internet with the function of security attached to cryptography that provides the maritime firms including shipping agents a faster means to validate crucial transaction

information thereby establishing trust in the supply chain. All these can be implemented in the shipping industry by way of helping in data search between different ports (Toll, 2020). It should be noted however that, all these advanced and novel technologies in the maritime sector that supports logistics and supply chains come with risks (Kianieff et al., 2019).

In embracing advanced and inter-linked digital technologies, the maritime sector is concurrently faced with an increase in cyber risk – a risk that exists in the cyberspace (Cheung & Bell, 2021). In 2017, AP Moller-Maersk, the Danish shipping giant was reportedly smashed by a ransomware known as NotPetya which made the company to lose finances in its logistics business to the tune of millions of dollars. In the same year, Svitzer Australia – one of AP Moller-Maersk's subsidiaries experienced a breach of their data through email accounts that were compromised such that they robotically forwarded mail to external accounts. These mails contained financial information that was sensitive (Cheung & Bell, 2021) Toll Group is another example of a third-party logistics service provider of Australian origin that was attacked by ransomware called Nefilim in January 2020 and subsequently in May 2020 by the same ransomware (Lennane, 2020). The European Union Agency for Network and Information Security (ENISA) has defined Cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets". According to this definition, it shows that for cybersecurity to be successfully implemented, it has to reside at the center of the governance process of a company management.

This study looks beyond this literature review and focuses on the measures aimed at improving cybersecurity in ports and the maritime logistics and supply chain.

2.4. Maritime Cyber Policy and Regulations

Up to the end of 2018, the world-wide enactment and implementation of sturdy policy for maritime cybersecurity was basically non-extant. The year 2013 saw the first assessment of maritime cybersecurity situation by the EU. It noted the international unawareness of maritime cybersecurity, the bias of existing policy towards physical

safety and security (European Union Agency for Cybersecurity, (ENISA), 2020). Not until recent cyber-attacks has there been the impetus to institutionalize prevention of maritime cyber-attacks(Gallagher, 2017) .

Today's world-wide maritime policies are developed by the International Maritime Organization (IMO) in 2018 - a United Nation's specialized agency responsible for regulating and governing shipping. The IMO works in partnerships with governments' transportation directorates, and other institutions for numerous shipping facets. The IMO, for example, developed the IMO International Convention for the Safety of Life at Sea (SOLAS) which evolved to The International Ship and Port Facility Security (ISPS) Code. The ISPS Code addresses a couple of cybersecurity concerns. For example, the requirement that every ship develops a cyber-security plan every five years.

Physical cyber-attacks

Cyberattacks and cyber-assisted attacks have now caused a sway in policy. Attackers abusing automatic identification system (AIS) to target ships is the most significant (Balduzzi, 2014). The IMO policies have become more stringent to the extent that they allow the masters of ships to turn off their AIS if it is known to make them vulnerable around piracy hotspots (International Maritime Organisation, 2011). While this policy is in place, technology improvements have made it possible to make anonymous or secure identity data instead of completely disabling the AIS. A good example of this is the UK Department for Transportation that provided guidance for the physical security with respect to piracy and other physical acts of violence against merchant shipping (Department of Transport, 2011) .

Cyberattack enabled by physical action

Because ships work remotely, there is a high likelihood of misassumption by management and stakeholders of the ship to be having reasonable cybersecurity. However, that security reduces in contexts where physical attacks overwhelm overtake on-ship physical security. Typical cyber hygiene for example deflects the connections of USB devices on most ship systems (BIMCO, 2016). However, a well-designed

policy adds flexibility without compromising security because devices require routine software updates yet rules may be ignored in favour of convenient software updates.

Mitigation Cyber policy

At the moment in almost all ports, there are business continuity policies to ensure operations after system failure. That notwithstanding, in the midst of a cyberattack, an inefficient system is not necessarily broken and a fully functioning system does not guarantee the provision of trustworthy data. On that account, operation and policies catalogue should account for these likelihoods, in lieu of just taking the system as one that is functional or non-functioning. It is important for one to understand this difference cyber-attackers can obscure the difference thereby causing confusion at both machine and human levels.

Prevention cyber policy

This segment describes the maritime cyber initiatives that can prevent cyber threats serves to rebuff the general maritime cyber defence approaches. Some of these proposed initiatives leverage previous sections e.g., cyber-physical security especially given the growing technologies that intersect with ancient, entrenched security at the physical level.

In thinking about future cyber-threats the researcher considers initiatives aimed at stopping and mitigating maritime cyberattacks. In particular, the subtle cyber-attacks. These are of interest for the near future in light of the evolution of maritime technology towards remote and autonomous operation. In addition to physical security that can be implemented at essential access points, there is need for policies for the interface of ship systems with other entities such as USB and SCADA. Such policies improve the capability of defending against continuous maritime cyberattacks. Such policies can be developed from existing proposals for cyber-hygiene as well as adapt from existing physical safety policies. This can be illustrated in cases where ships always have navigation systems that are redundant such as SONAR or ECDIS (*ECDIS: Navigation in 2018,* 2018).

It should however be noted that it is paramount from the perspective of cybersecurity that systems that are identical do not share same vulnerabilities owing to the risk of failed protection against deliberate cyberattacks yet seemingly protecting against accidents.

The IMO resolution A.1079 (28) insists that crews must be trained thoroughly and adherence emphasized when conducting any training programs on policies related to cyber awareness; ship interaction with systems ashore; segregation and clarification of duties for specific OT and IT systems; and alert mechanisms for cyber incidents or issues. The International Electrotechnical Commission (IEC) 62443 and 61508 standards require compliance with these standards in designing cyber-security alarms in the context of the safety of ships and the controlling of ships. In addition, the International Organization for Standardization (ISO) 27000 document series require that security policies for onshore management security alerts at office-level must be aligned with ISO 27000

Considering existing standards of classification of system vulnerabilities cyber-physical, cyber vulnerabilities narrated in here allows for a more robust and effective policy-assembling process in comparison with the previous cyber-hygiene reports (NOSAC 2016) and (IET 2017).

In conclusion therefore, the maritime industry is clearly a late adopter in comparison with other sectors when it comes to ship and shore infrastructure security, both of which are critical national assets. The maritime industry should therefore embrace and adopt new perspectives to regulation and training in the short to medium-term while considering the setup of modern systems in the long term. Cyber policy design, additions and amendments are known to avert, mitigate and defend from undesired cyberattacks and their related outcomes in the maritime world. These policies can have a positive as well as significant bearing in present-day contexts in battling cyber threats that are known and some that have not yet occurred.

CHAPTER 3: METHODOLOGY

3.1. Introduction

To meet the objectives and address the research questions, a case study and a qualitative research methodology was used owing to its ability to leverage and investigate multiple disciplines and concepts. A qualitative research design emphasizes meanings and processes that are not investigated with respect to amounts, frequency or quantity. The researcher chose this methodology because it provides insights into the maritime cybersecurity practices of two cases – Spain and Kenya – in an attempt to understand the social and policy dimensions that distinguish developed countries and developing countries in the implementation of maritime cybersecurity practices. Qualitative research leverages a contextually responsive data collection and case analysis approach thereby providing a holistic conceptualization of the research questions/phenomena.

The researcher chose a qualitative design so that maritime cybersecurity practices can be examined in their natural environment as well as with respect to what the research subjects interpret their context to be (Eriksson & Kovalainen, 2008). The researcher chooses a case study because it shall efficiently provide insights into how cybersecurity is seen in practice in line with (Rashid, Rashid, Warraich, Sabir, & Waseem, 2019) who argue that case studies are an efficient research approach in answering research questions that require understanding of specific research phenomenon and their practical manifestation. This allows a historical, technological, social, economic and cultural investigation of the research questions as well as an objective observation of the phenomena – in this case maritime cybersecurity practices (Eriksson & Kovalainen, 2015).

A case study provides for the investigation of one or more phenomena, and as (Teegavarapu et al., 2009) argue, it can involve investigating a whole system or parts of a system, an economy, a process, an organization or a structure.

3.2. Research Scope and Activities

Research Scope

The researcher limited the study to maritime cybersecurity in port operators and shipping. Other sources of information shall include news, publications and journal articles describing maritime cyberattacks and maritime cybersecurity.

Figure 3.1: Research Activities

The study underwent the following exercises:

Exercise 1 - Study scope definition and identification of experts: step number one of the study involved establishing the project scope and selection of experts on matters of cybersecurity. Their input was captured and reflected upon in drafting of the dissertation. These experts included port personnel and respective stakeholders responsible for cybersecurity, state officials as well as other third parties/stakeholders.
Exercise 2 – Desk and Online research: In this phase/step, the researcher conducted a search for recent, relevant literature in line with the study subject. The sources were referenced and linked to other sections of the dissertation including the development of good practices and recommendation.
Exercise 3 – A series of interviews using semi-structured questionnaires were carried out with the Subject Matter Experts (SMEs): The questionnaires reflected maritime cybersecurity components which were filled in by six maritime-ecosystem stakeholders from Valencia and Mombasa Port Authorities. The respondents included security, cybersecurity, OT and IT managers, as well as a representative of each study country's national ICT and cybersecurity agency).
Exercise 4 – Data analysis and report-writing: the data collected through online and desk research and the subsequent interview responses were analysed. Findings were

identified, documented and were used in drafting the dissertation as well as the preparation of the final document.

Exercise 5 – Review and subsequent validation of the dissertation: This dissertation was reviewed and underwent validation with maritime cybersecurity and other SMEs by way of sharing of the draft dissertation as well as obtaining comments and feedback.

3.3. Data Collection and Analysis

Data Collection

Data collection for this case study leveraged a variety of sources including:

- Documents, archives, publications, journals, reports, and, research literature/articles, news articles,
- Participatory observation, and
- Interviews

The case study shall use one or more of the above-mentioned data sources. Leveraging on the flexibility of the use of various sources of information in a case study, the researcher shall use data triangulation so as to get a comprehensive view of the maritime cybersecurity practices in developed and developing states. This shall enable the researcher to come up with credible and valid research results and findings (Marshall & Rossman, 2014).

Data Analysis

Data analysis aimed at providing clarity on the research questions as well as identify areas for further investigation. The data collected from the study was then subsequently analyzed using Colaizzi's 1978 framework for qualitative data analysis where the data collected was coded into themes reflecting the research questions (Marshall & Rossman, 2014) and analysed by comparing and formulating logical perspectives. The researcher thereafter interpreted the results by debating them, deriving logical conclusions and clarifying comparisons with research literature. In this regard, the maritime cybersecurity practices of Spain and Kenya was compared in order to establish the similarities and/or differences between them with regard to their implementation.

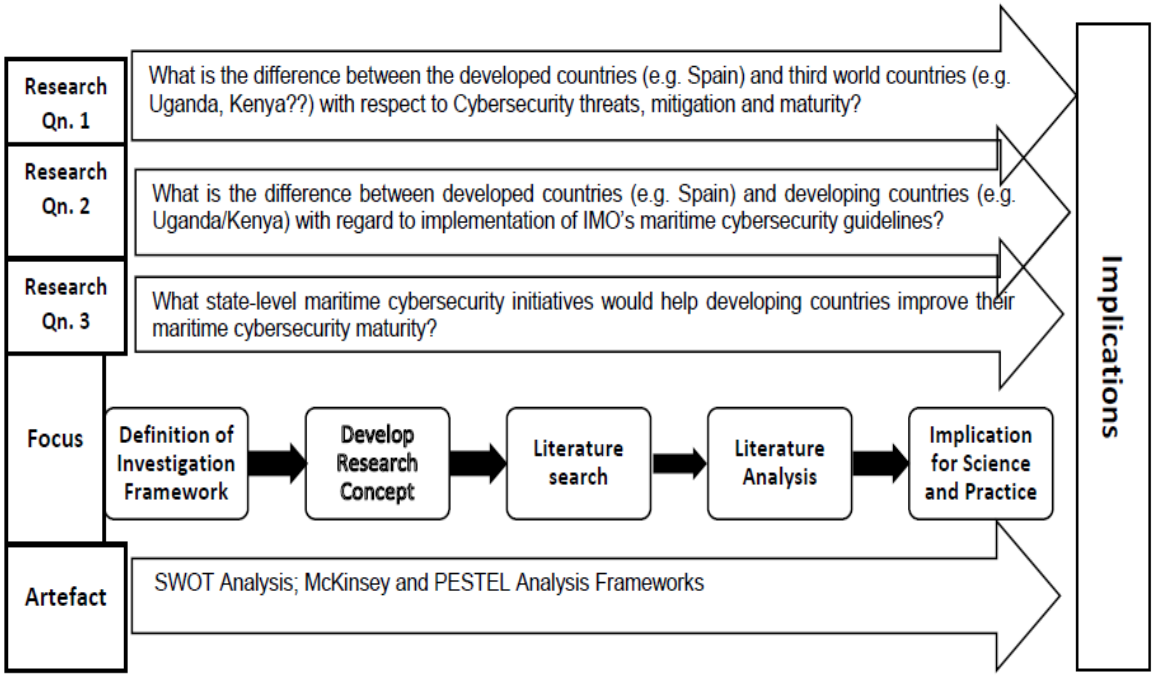

Figure 3.2: conceptual framework for systematic analysis of literature (Adapted from: (Vom et al., 2009)

3.4. Description of Colaizzi's Framework for Qualitative Data Analysis

Colaizzi (1978) outlined a qualitative data analysis process with seven phases. This analysis allows for alignment of the different phases with the raw data thereby providing a brief and exhaustive description of study phenomena that is subsequently validated by respondents that were used to generate this data (Morrow et al., 2015). Qualitative data collection leverages first-hand, personal narratives of respondents' experience. This can happen through in-person interviews (online or face-to-face), written accounts of respondents' experiences, reviewing personal blogs or using research diaries. The stages are as shown below:

Table 3.1: Colaizzi's Framework for qualitative data analysis(Morrow et al., 2015)

Framework for Qualitative Data Analysis	
Phase	**Description**
1. Familiarization	Researcher reads through all information from respondents more than once, to familiarize oneself with the data
2. Identification of statements that are significant	This involves identifying and taking note of key and relevant statements in relation to the concepts or constructs under study
3. Formulation of meaning	After careful reflection, the researcher attaches meaning to the data. These meanings must be closely aligned with the construct or concepts under study and the experience of the respondents while at the same time eliminating the researcher's assumptions (However, Colaizzi (1978) observed that complete detachment from the context is impossible).
4. Clustering of data into themes	This phase involves grouping of meanings identified by the researcher into cross-cutting themes as reflected or represented across the responses. The elimination of assumptions and presumptions by the researcher enables avoidance of any influence of theories already in place.
5. Develop a comprehensive description	A detailed description of the concept or construct is developed in this phase. It should reflect all the themes identified in phase 4.
6. Develop a central message or structure	By condensing the comprehensive description, the researcher is able to reflect and capture aspects that are considered core to the structure of the concept or construct.
7. Validation	A validation process involves taking the derived central structure of the concept or construct back to the

	research respondents to see whether it adequately reflects their experience. This process is iterative (from the start to this phase) depending on the feedback the researcher gets regarding the alignment of the findings with the respondents' perception of adequate representation of their issue.

3.5. Description of the McKinsey 7S Model

The McKinsey's 7s model, developed in the 1980s and widely used by practitioners and academics aims at emphasizing the human (or soft) skills in comparison with infrastructure, equipment or capital. It remains popular as a strategic planning tool and has been considered as an important driver of organizational performance (Mindtools, 2020). The model demonstrates how 7 elements - Structure, Strategy, Skills, Staff, Style, Systems, and Shared values – of organization, can be leveraged to drive organizational effectiveness.

The McKinsey's 7S model provides a robust framework for reflection on organizational infrastructure, activities, and interactions.

Figure 3.3: The McKinsey 7S Model

The following is the definitions of the elements:

Strategy–Describing the alignment of organizational resources and capabilities to "succeed" in its operational environment.

Structure–A description of the structuring of the organization including reporting relationships, role definitions, and descriptions of key responsibilities.

Systems–The technical and business -related infrastructure leveraged daily by staff to deliver organizational performance.

Shared Values–The set of beliefs of the organization as described in expected traits, behaviours or characteristics in addition to the organization's vision and mission.

Style–The organizational leadership behaviour and cultural components.

Staff–The staffing plans, worker base, and talent management practices.

Skills–The existing staff ability to perform in the organization, which manifests in organizational performance.

3.6. The PESTEL Framework

PESTLE analysis model analyses the macro environmental factors that may significantly impact organizational performance. PESTEL is derived from: Political, Economic, Social, Technological, Environmental and Legal factors (Salem, 2018). This model is used alongside another SWOT analysis tool that is used to document threats and weaknesses, strengths and opportunities (Sheffield Hallam University, 2019). While this framework has been found helpful for start-ups or those making entry into foreign markets, the PESTEL analysis tool works best when used alongside other frameworks such as the SWOT analysis and McKinsey 7S model for a clear comprehension and interpretation of internal and external organizational contextual factors. The PESTEL framework has over time been expanded to include Demographics, Ethical, Intercultural, and Ecological factors thereby evolving with acronyms like DESTEP and SLEPIT. In this dissertation, the researcher will simply stick to PESTEL because it reflects the core factors in business. The PESTEL factors are elaborated as below:

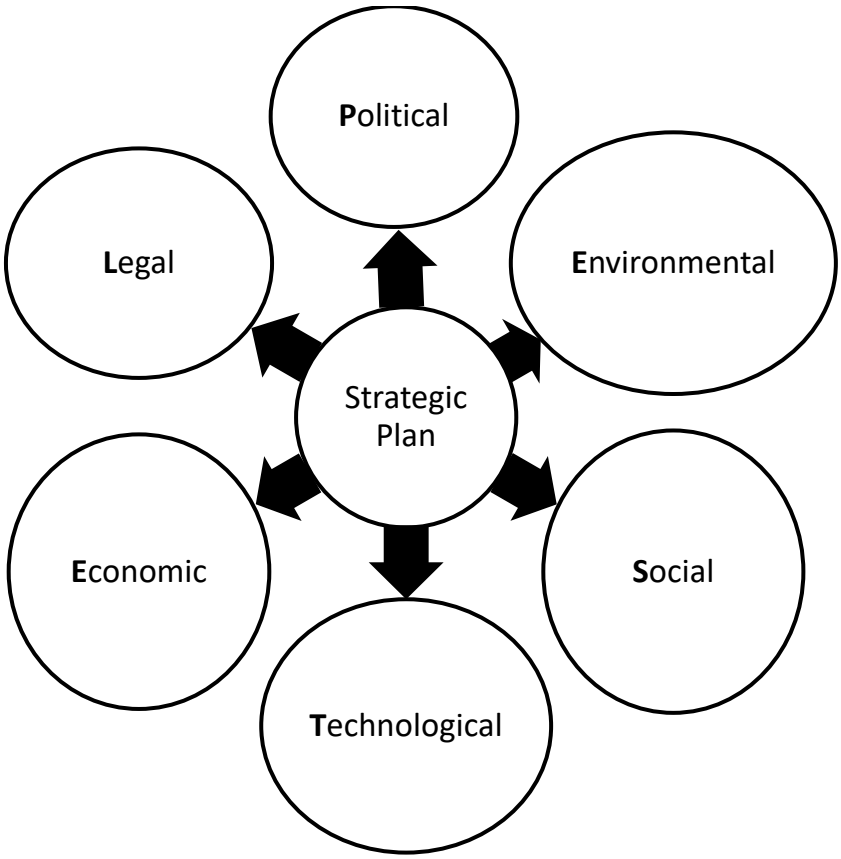

Figure 3.4: The PESTEL Framework

Political Factors–This refers to the degree of government intervention within the economy.

Economic Factors–presents a considerable footprint on how an organisation does business, together with how flourishing they're.

Social Factors-This is usually mentioned as socio-cultural factors; it includes the population's shared belief and attitudes, together with – population growth, age distribution, health consciousness, career attitudes and then far more.

Technological Factors–This is understood to have an effect on the flexibility of a company to promote, build, and ship product and services.

Legal Factors–A number of legal factors can affect the ability of an organization to operate.

Environmental Factors–There are industries that are sensitive to environmental changes including maritime, tourism, agriculture, and farming. The issues here are;

weather, climate change, and geographic location which might influence a company's business decisions

3.7. Description of the SWOT Analysis Framework

SWOT is a short form for Strengths, Weaknesses, Opportunities and Threats. Strengths (S) and Weaknesses (W) are the internal factors over which an organization has a form of control while Opportunities (O) and Threats (T) are as external factors over which an organization does not have complete control (Gürel, 2017). SWOT Analysis has been used to analyze organizations' strategic positions in the context of it internal and external environment. It helps users identify the strategies that lead to the development of a firm-specific business model at optimal alignment of resources and capabilities (Tanya & David, 2015).

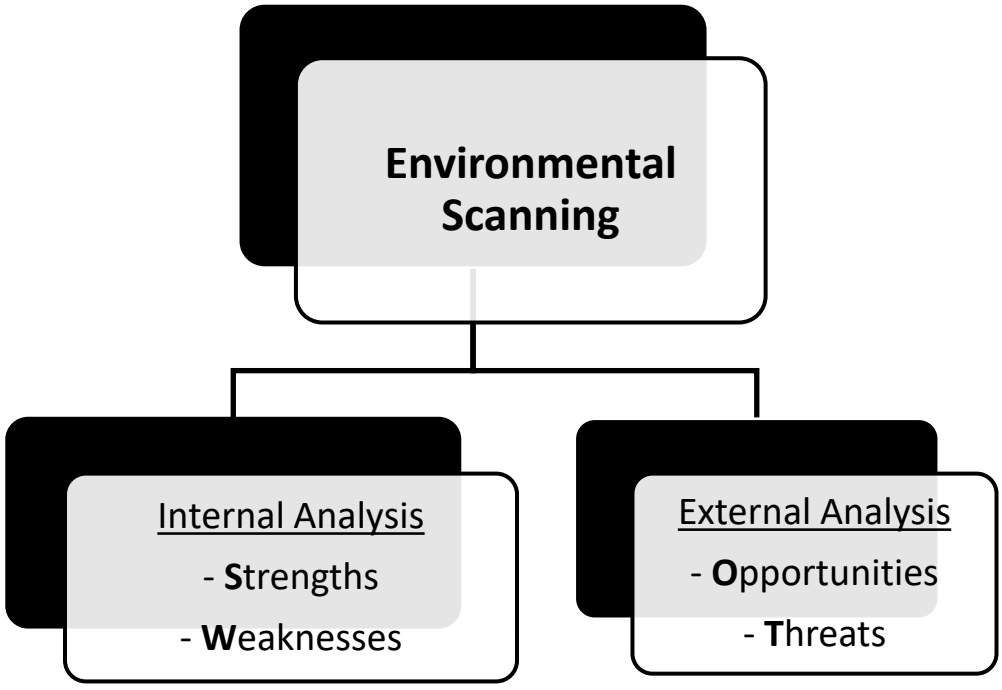

Figure 3.5: The SWOT Analysis Framework

Below is the overview of the four factors (Strengths, Weaknesses, Opportunities and Threats) –

Strengths - These are the qualities that enable us to accomplish the mission of the organization.

Weaknesses – These are the qualities and characteristics that stop us from conquering our mission and achieving our full potential. These factors dwindle influences on the success and growth of the organization.

Opportunities - These are presented by the environment in which our organization operates. They come about when an organization can reap the benefit of conditions in its environment to execute and plan strategies that propels it to become more successful.

Threats – These happens when conditions in the external environment ransacks the dependability and success of the organization's business. Threats cannot be controlled and when they come, the steadiness and survival is placed at stake.

In summary therefore, SWOT Analysis is quintessential in the formulation and selection of strategy. It is quite an excellent and powerful tool, however, it pertains a great subjective element. For maximum benefit, the tool is better used as a guide, and not as a prescription.

CHAPTER 4. MARITIME CYBERSECURITY IMPLEMENTATION IN DEVELOPED AND DEVELOPING COUNTRIES

4.1. International Maritime Cybersecurity Perspective

Globally, by 2002, the International Ships and Port Facilities Security Code (ISPS) had been embedded into the Safety Of Life At Sea (SOLAS) Convention. It was aimed at identifying the marine security-related roles of port facilities and articulating their compliance obligations.

This ISPS Code necessitates the planning of a Port Facility Security Assessment by ports by determining major assets, possible threats and countermeasures. This, in addition to a Port Facility Security Plan that outlines measures, actions and assumptions made in ensuring port security. The PFSA is expected to take into consideration procedural policies, physical security, systems that protect personnel, structural integrity, telecommunication and radio systems, computer networks/ systems as well as critical marine transport substructures. In addition, the PFSP should be able to cover access to the port facility, restricted areas' management, freight handling, ship's stores delivery and port facility security observation.

The Facilitation of International Maritime Traffic (FAL17) and SOLAS resolutions outline how information exchange between ports and third parties should be carried out. This exchange, described in nine different but consistent approaches has been mandatory since April, 2019. The standardization of data exchange has impacted the ports' IT ecosystems thereby introducing additional IT security challenges. This is because Cybersecurity in maritime systems, specifically ships only garnered International focus from about 2017 yet being manifested through recommendations at a global level on how maritime systems should be secured.

Maritime Cyber-risk management has been articulated in IMO guidelines by The International Maritime Organization Facilitation Committee and the Maritime Security Committee in the MSC-FAL.1/Circ.3 19 with the call for increased cyber risk awareness as well as key maritime cyber risk management recommendations ranging from current to future cyber risks. The guidelines articulate and distinguish Information Technology and Operational Technology systems.

4.2. Maritime Cybersecurity in Europe Vs. Africa

4.2.1. Spanish (EU) Maritime Cybersecurity Policy Overview

EU regulation affected the organization of the maritime ecosystem, subsequently affecting ports in the areas of security, safety, and data exchange.

The EU can be argued to have adopted and utilized some components of the SOLAS Convention in a number of related rules and regulations (EC) 725/2004 (NIST, 2018). For example, one that focuses on enhancing the safety of ship and port facility and the implementation of the Code of International Ship and Port Facility Security (ISPS). On the other hand, the Directive 2005/65/EC(European Union, 2005) focuses on enhancing port security while Regulation (EC) 336/2006 dwells on the International Safety Management Code (ISM) implementation among the European Union maritime sector. Nonetheless, the philosophy code isn't applicable to ports. Directive 2010/65/EU (European Union, 2010) requires Member States' ports to utilize standardized forms in order to ease traffic. This directive additionally requires that SafeSeaNet systems be established at country and global level thus to facilitate secure exchange of knowledge between maritime authorities of Member States and alternative authorities' systems like customs systems. Directive 2005/65/EC and Regulation (EC) No 725/2004 are the noted legal frameworks that support security plans and risk assessments for ports and their respective facilities. In implementing this directive, the Member States are expected to draft a PFSA while the Port Authorities concurrently set up their PFSP such that approval is attained prior to implementation by the Member States, who are responsible for monitoring the implementation of the PFSPs.

The European Maritime Security Strategy (EUMSS) was developed in 2014 and subsequently revised in 2018 by the European Union. It is a shared and comprehensive tool to monitor and respond to the protection of activities of the individuals and assets of the maritime system. For ports, the revision of the EUMSS, that was consequently adopted by the overall Affairs Council on 26 June 2018, aimed at centralizing coverage to boost awareness and healthier follow-up to the policy and strategy. In addition, the Regulation (EU) 2016/679, referred to as the general data Protection Regulation

(GDPR) – introduced in 2016, which covers the protection of privacy in light of the movement of information. The GDPR details necessities for private information protection and applies to all essential sectors including the maritime sector.

Essential services Operators known within the system of water transport as described by the EU include the following:

Inland, ocean and coastal travellers and freight water transport corporations as outlined in Appendix I of Regulation (EC) 725/2004. It however, does not cover the specific vessels operated by those companies;

Management of ports: includes "any gazetted space of land and water, with boundaries outlined by the Member State within which the port is set, containing works and equipment designed to facilitate industrial maritime transport operations" as per Directive 2005/65/EC. This includes port facilities as well as equipment and works operators in the ports.

The EU Cybersecurity Act was established in 2019 to strengthen the position of ENISA within matters of cybersecurity for the member states of EU. It defines certification framework for cybersecurity covering ICT product, services and processes for the EU bloc. This framework provides for a set of standards, rules, technical necessities, and procedures ensuring that ICT services and products are reliable reflect the needs of the EU.

4.2.2. African Maritime Cybersecurity Policy Overview

According to (Reva, 2020), the future development objectives of Africa assume fully operational ports and shipping sectors with no clear articulation of the cybersecurity component. This unfortunately leaves them open to cyber breaches and disruptions. Whereas cybersecurity in Africa is gradually becoming acknowledged as an essential element of maritime security, its incorporation into African maritime security apparatuses and frameworks is not being accelerated, which is not. However, these sectors are currently being faced by a number of challenges connected to efficiency and effectiveness, including their repeated transformation and innovation is dire if the socio-economic needs of Africa are to be served.

Given that cybersecurity is not specific to one country, this gives the African Union (AU) a leading role to facilitate member state's maritime security capabilities. In 2014, the African Union made a positive start by adopting the Malabo Convention - Convention on Cyber Security and Personal Data Protection and the organization also incorporated cybersecurity as a leading initiative in its Agenda 2063 plan.

The Institute for Security Studies (ISS) argues that cybersecurity is rapidly becoming an important chunk of the maritime security needs of Africa, therefore requires shared action from African states given the rapid digitalisation that will make Africa's maritime infrastructure a high-risk target.

This hard work will not yet be sufficient to defend Africa from the varieties of maritime cyber-attacks that is continuously being reported in other parts of the globe. There was a prominent occurrence when the ICT systems of the International Maritime Organization (IMO) were attacked, rendering the IMO's website unusable and totally shut down for two days but no serious impairment was stated.

4.3. Implementation of Maritime cybersecurity: Best Practices

Globally, the increasing digitalisation has led to new policies and laws that require ports to deal with new challenges brought about by ICTs. Ports' reliance on novel technologies for increased competitiveness, are expected to observe some standards and policies as they enhance operations. As a results of this, new stakes and challenges in cybersecurity arises, each within the information Technologies (IT) and Operation Technologies (OT) worlds.

The implementation of policies and standards permits the identification of measures that ports will then enact to better shield themselves from cyberattacks. A number of known measures are outlined in the contexts that follow. They are meant to function as sensible practices for individuals like CISOs and CIOs that are in charge of the implementation of cybersecurity in Port Authorities and Terminal Operators.

4.3.1. Port of Mombasa (Kenya)

The Kenyan government has brought in a number of steps in trying to solve the increasing cyber threat. The National cybersecurity strategy of Kenya, developed by Kenya's Ministry of Information, Communications, and Technology in 2014, comprises four primary objectives. Number one - to protect "critical information infrastructure." Number two - to promote awareness of cybersecurity by "informing and educating the Kenyan public and workforce." Number Three - to set up a cybersecurity framework that nurtures collaboration and reduces "duplication of effort." And lastly - to make sure the strategy is effectively implemented to the letter and updated to adapt to the evolving threat environment. Additionally, in 2017, Kenya established the National Cyber Command Center also known as known as NC3 to forefront and coordinate national efforts to cybersecurity. The NC3 works with public – private and not-for profit partnerships.

4.3.2. Port of Valencia (Spain)

The port of Valencia has a robust cyber security governance framework at port level that incorporates all port operations' stakeholders. These stakeholders include Port Authority, port operators, pilotage company and shipping corporations.

It is critical that all the stakeholders concerned with matters of cybersecurity are engaged and are willing to participate in the worldwide port operation security. The port of Valencia is taking varied steps therefore to raise its cybersecurity including:

Raising awareness regarding port-level cybersecurity, developing a culture of cybersecurity. While the port is traditionally meticulous when it comes to safety and security matters, it seems cybersecurity has not been absolutely assimilated within the minds of stakeholders. This step is combined with coaching could therefore, guarantee a shared understanding of cybersecurity and the potential to use it in daily processes.

Enforcement of cybersecurity measures includes segregation of network, countersign hardening, updates management, segregation of rights among others. Within the space of OT involving legacy systems that cannot be updated in most cases, network segregation and countersign protection are crucial to ensure an optimum level of cybersecurity.

The port considers security intentionally in applications, most notably because the port utilizes variety of systems whereby some are accessible to third parties for information exchange which can cause compromise of the port systems if there is any vulnerability. Enforcement of early detection and timely response capabilities at port level mitigate in real time any cyberattack before it affects the operation, safety and security of the port. The port depends on simple measures of detection like alerts once a particular action is completed.

CHAPTER 5. CASE STUDY OF KENYA AND SPAIN

5.1. Cybersecurity Implementation at Mombasa Port

5.1.1. Overview of Mombasa Port

Mombasa port is notably of the oldest harbours in Africa. It dates back as early because the eighteenth century. The port is found on the lineation of Republic of Kenya and it serves a big rural area of nearly 250 million individuals comprehensive of from Republic of Uganda, Kenya, Rwanda, Tanzania, Burundi, Republic of Congo, Northern jap Democratic, South Sudan, and African nation. Mombasa port is managed by Republic of Kenya Ports Authority (KPA) that could be a state corporation whose major goal is to facilitate and improve maritime trade by providing competitive services. The port has 2 instrumentality terminals that is; the Mombasa instrumentality terminal and therefore the Kipevu instrumentality terminal, that has created the port to register noteworthy growth in volumes of traffic over the past decade. The annual loading turnout has been increasing by 6.9% and therefore the instrumentality traffic mounting by 9.3%, as noted by the ports authority (Kenya Port Authority, 2015). Figure 6.1 provides an outline of the map of the port of Mombasa showing the road connections to the enclosed port space, the berths, and put in beacons & buoys.

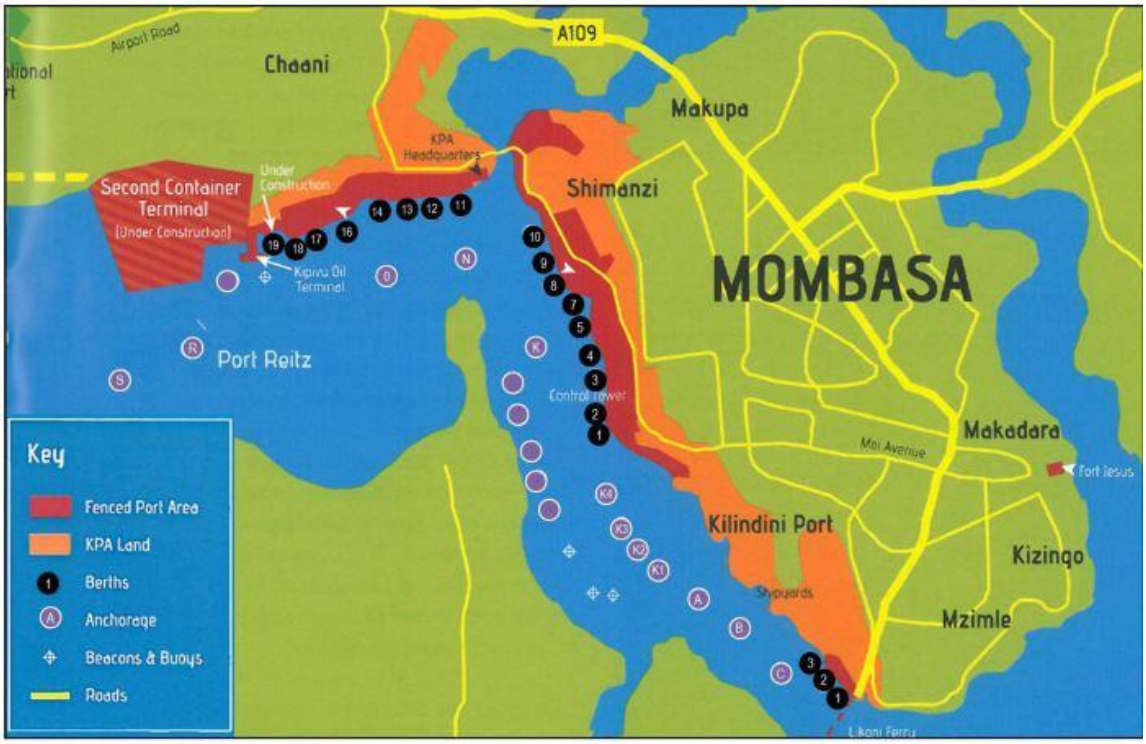

Figure 5.1: The overview map of Mombasa Port, Africa ports(Trevor, 2021).

5.1.2. Cyber Risk and Threat Management at Mombasa Port

General Cybersecurity risk and threat mitigation practices at Mombasa Port

Mombasa Port Employees

Senior leaders and Risk Officers at Mombasa port are taking time to define what their desired (Cybersecurity) risk culture should look like and what steps they can take to promote and maintain this at all levels of the port although this seems to take forever. However, the focus is found to be solely a "tone from the top" attitude instead of an inclusive embedding of values and daily behaviours at all levels and strategy. Many port employees including risk officers interviewed seem to acknowledge the slow and inconsistent steps taken to address this risk as noted by respondent #MOM05—"while progress has been made by this port, embedding cybersecurity risk culture throughout the port still remain a key challenge for many years to come". He was defensive by saying — "cultural change however does not happen overnight." Respondent

#MOM03 added to this by noting— "I have never heard or seen the CEO or CRO communicate the importance of Cybersecurity risk management and instil a risk management culture at all levels of the port". Cybersecurity risk management is not embedded into all spheres of the port.

The port uses incident investigation, auditing, and Internal Communication and Periodical Reports in identifying Cybersecurity risk. From this view, it can be noted that the port leaves behind very important Cybersecurity risk identification approaches including Industry Benchmarking, risk survey, Inspection by the port risk staff, Incident investigation, and brainstorming. The port also uses strategies such as Business Impact and Threat Analysis, SWOT (Strength, Weaknesses, Opportunities, Threats) Analysis, and Business Continuity Planning to analyse risk. This is however known not to be comprehensive enough to make a summative risk analysis. Important strategies such as PESTLE, BPEST and Research and development is left out.

The port is also establishing a fairly better internal controls and documentation in the area of Cybersecurity risk management although it is not enough:

> From now on, we are focusing not only in continuing to improve our ability to manage Cybersecurity risk but also more importantly, we are trying to improve our capacity that can demonstrate our efficiency in Cybersecurity risk management by way of documentation and reporting... we are setting parameters to achieve that as we speak. ——Respondent #MOM01

The port reports of using a handful of measures to identify Cybersecurity risks including; internal communication, periodical reports, general risk reports, Cybersecurity systems auditing, and incident investigation. The port also uses methods like market survey, business impact and threat analysis, and Business Continuity Planning to make Cybersecurity risk analysis.

The port reports of planning to spend a reasonable amount in their budget towards digital transformation. According to one executive, Respondent #MOM05 "we intend to invest a mouth-watering amount towards technology in our 5-year plan beginning 2021/22. This shall include investments in the latest hardware and innovative maritime products-both hardware and software." Asked to clarify what amount or what percentage of the yearly investment budget this will take, he quickly responded "the details are not yet available as I speak but will be … in a few weeks."

Digitization of core business functions and processes is being taken by the port including the digitization of sales and marketing, human resources, IT/OT, etc. However, there is limited and less efficient risk management information systems in place and yet the standard goes ‘as ports digitize, so must risk’ because it is becoming increasingly common that ports are no longer “owning” the client interface because of digitization. There is a strategic plan on increasing spending a high amount on digitization of business processes and functions in the next few years even though specifics were not delved into.

Although the "culture at the top" at the port shows support for Cybersecurity risk management through policy documentations, senior management is found to be less informed and concerned about Cybersecurity risks and mitigating controls as noted by one Respondent #MOM09:

> All through board meeting of which I sometimes attend, when the issue of technology and Cybersecurity related risks are brought up, there is little support or concern for it. This makes me to always tend to keep the issues down to my department and not bring it up to the top guys inform of email, memo or whenever there is a meeting.

Cyber Systems risk and threat mitigation practices at Mombasa Port

Mombasa port now, more than ever, rely on IT/OT to spur growth by identifying opportunities. For IT/OT systems to play a pivotal role in business transformation and growth in the industry, proactive IT/OT systems risk management approach need to be practiced. IT/OT systems risk management, as a part of operational risk management in a port need to revolve around seeking answers to some pertinent issues relevant to the port. This sub-chapter presents the various approaches being taken by Mombasa port in managing IT/OT systems threat and risk.

Mombasa port Employees

Backups at the port are used for complete IT/OT system restoration. Backups are also extended to saving more than just digital data. Backup processes include the backup of IT/OT system specifications and configurations, policies and procedures, equipment, and data centres. Back up is always done by the Database Admin or System

Admin. The port however, is not using alternatives to traditional backups, such as redundant systems and cloud services. One situation that was explained by Respondent #MOM08 was that "There was a backup that was not good, another situation, the backup media was damaged, and we could not easily fix the problem." Just having a backup procedure in place does not always offer adequate protection, he concludes.

Security Organization: The port maintains a fairly safe circle of IT/OT security practices. These include; User Authentication-all employees within and without a port uses one or a combination of the following; Something he/she knows (a password or PIN), Something he/she has (a card or token), Something he/she is (a unique physical characteristic). According to the researcher's experience, not all the employees are availed with a combination of these security elements. Respondent #MOM08 concurs "I have a secret password for some systems but not a card or biometrics for accessing even basic rooms at the port." All security complaints and problems are reported to the ICT manager and then to the CIO.

Application Security: The port employs both network and computer-based control of applications. Respondent #MOM09 had this to say:

> we do control applications on the network, by allowing or denying the network connections required for the applications to communicate. We also control the computers on which the applications including Cybersecurity application run, by restricting which applications can be run on computers and we control what functions each application is allowed to perform through policy templates.

Network Security: The port uses a combination of security mechanisms to secure its network including using routers and switches to increase the security of the network, Virtual Private Networks (VPN), unified threat management platforms (firewalls combined with network antivirus, web filtering, IPsec, and other network-oriented security functions). The port however does not perform application network communication control, advanced wireless network hardening practices and this is found to be a serious security concern. The port also presents shaky security practices for Voice over IP (VoIP) infrastructure.

Physical Security: The port carries out a number of measures to ensure the physical security of IT/OT infrastructure including; classification of assets which is the process

of identifying physical assets and assigning criticality and value to them in order to develop concise controls and procedures that protect them effectively, building access control systems, mantraps at the entrance (an area designed to allow only one authorized individual entrance at any given time), locks, bugler-proof doors and file cabinets, laptop locks and docking stations, controlled access to data centres, wiring closets, and network rooms, building and employee IDs, biometrics, security guards, physical intrusion detection (for example. Closed-Circuit Television-CCTV, alarms).

The port is integrating old legacy systems with modern solutions in an endeavour to modernize their systems. This however, has been a huge hassle for the port in the process of seeking to improve Cybersecurity.

> Legacy hardware here is a difficult issue to handle. They are cumbersome, unruly, and challenging to update and manage. Most of the outdated infrastructure at the port are struggling to keep up with the demands of modern solutions, creating a bottleneck for Cybersecurity processes and operating capacity —— Respondent #MOM05

One of the challenges is that some of the modern cloud and other SaaS solutions are incompatible with the older legacy systems. This means that in order for the systems administrator incorporate new tools and programs, extensive custom code is required to make it work. This has resulted to the emergence of data silos at the port, whereby different departments across the port cannot freely access the data they need.

Maritime Industry Practitioners

Mombasa port functions in an ever changing operating setting characterised by rising prospects from the customer with an ever changing landscape of the economy, enlarged scope and strength of regulations for industry. It is leveraging less of technological innovation geared towards IT/OT systems risk management, while at the same time staying less vigilant against evolving IT/OT systems risks.

> While the count of remote incidents of one-time failures in Cybersecurity has come greatly reduced, active IT/OT risk management at the port has tripped. This setback is majorly attributed to insufficient Cybersecurity risk information and a reactive rather than pro-active IT/OT risk culture. Respondent #MOM02

5.1.3. SWOT analysis for cybersecurity strategy implementation at Mombasa Port

This sub-chapter is a SWOT analysis of the Mombasa Port which will later specify strategies that the port should implement to make it cyber secure and competitive. This SWOT analysis is a method of reviewing the current cybersecurity mission of the port as well as defining a new one. The aims at examining the strengths and weaknesses related to the internal review of the port as well as the opportunities and threats to review the external environment of the port.

Table 6.1: SWOT analysis for cybersecurity strategy implementation at Mombasa Port

Cybersecurity Strategy Mombasa Port Implementation

INTERNAL FACTORS	
STRENGTHS (+)	**WEAKNESSES (–)**
1. Easter Africa Trade route 2. Biggest port - container capacity in East Africa 3. Favorable dwell time as compared to other ports in Africa 4. Well established port infrastructure 5. Good port productivity 6. The port is favored by both cargo owners and shippers 7. Good road and rail connections 8. Close proximity to manufacturing bases 9. Although Mombasa port has problems in regard to modern equipment and their availability, the turn	1. The port is highly congested 2. The roads to the hinterland is highly congested 3. There is very poor Utilization of rail at the port 4. Prices at the port is so high 5. Less IT and OT Infrastructure compared to international ports 6. Mombasa port is restricted in its activities because it is government owned.

		round time for vessels is very promising and competitive compared to other ports in Africa 10. Mombasa port has very good financial returns.	
EXTERNAL FACTORS	**OPPORTUNITIES (+)**	**STRENGTHS (+) / OPPORTUNITIES (+) STRATEGY**	**WEAKNESSES (–) / OPPORTUNITIES (+) STRATEGY**
	1.Presence of Mombasa dig-out port 2.Presence of support services for East Africa oil and gas reserves 3.Increase in the transit of bulk commodities along the corridor 4.The hub port of the East African Community region 5.Development of the dry ports in Kenya, Uganda, and Rwanda 6.Freight and logistics cost reduction through improved productivity and efficiency	Provision of strategic, tactical and operational measurements in focus of the systems perspective; Product and Service development; Provision of value-added services for cargo and vessels for reduced costs for vessels and cargo; Business Requirements Analysis; Downsizing and/or specialising leading to market focus and cost reduction; Creation of Alliances and Partnerships.	Open and Integrative Organization structure; Free Port Status for Free Trade Zone for market focus, Reduced Cargo Costs; Upgrading labour skills to increase efficiency and capacity; Reduction in labour requirements to increase in efficiency; Provision of multidisciplinary skills; Enhance managerial skills in leveraging resources and translating strategic intent into actions for work groups; Creating learning environment by providing time, space and resources, visibly recognize success.
	THREATS (–)	**STRENGTHS (+) / THREATS (–) STRATEGY**	**WEAKNESSES (–) / THREATS (–) STRATEGY**

	1. Competition from other east and southern African ports such as Durban (South Africa), Bagamoyo (Tanzania), Techbanine (Mazambique) 2. Economic slowdown of the East African Economies especially due to COVID-19	Additional sites of Cybersecurity Infrastructure to increase capacity and location. Management Reorganisation for overall efficiency to reduce operating costs; Closely integrated research and development.	Development of new facilities to Increase in efficiency, throughput and capacity; Acquisition of new equipment; Development of systems including control systems, recruitment and selection systems, innovation management information systems, competitor analysis, Appraisal, training and development systems, and recognitions systems.

Upgrading of the general port infrastructure including the IT and OT infrastructure which provides access to other ports has augmented attractiveness of the port for investors as well as maritime and land carriers. A much higher growth in handling performed by the port in comparison to what was anticipated in the diagnostic documentation on which Transport Development Strategy is founded approves that the position of the ports in the African port market is strong. Even though the port has glitches in relation to modern infrastructure and their availability, the despatch time for vessels is very encouraging and viable in relation to other African ports.

Opportunities are potential areas in which the port can identify potential growth, profits and market share and for Mombasa port it includes new lines of business in developing markets. There is growth of international trade which has opened up business opportunities for the port to open new lines of business in markets in developing countries whose booming economies demand more and more products of a high level and price including technological products. Additionally, digitalization makes it possible to manage goods and passengers more efficiently, leading to the transportation of more volume together, preferential of the scale factor, thereby improving competition.

5.1.4. GAP Analysis: McKinsey 7-S Framework and PESTEL.

The McKinsey framework is founded on the basis that a port consists of seven critical facets. The study sought to analyse and establish the cybersecurity strategy implementation of Mombasa port and that it has yielded to the concept in order to realize their objectives. The results are presented in the Table 5.2.

Table 5.2: Mombasa Port Cybersecurity Strategy Analysis using the McKinsey 7s Framework

McKinsey 7S Framework	**Complies**	
	Yes [05]	***No [0.0]***
STRATEGY		
• Involvement in the cybersecurity strategy formulation		***N***
• Simple, clear, and easily understood cybersecurity strategies	***Y***	
• Concise cybersecurity implementation stages and timeline		***N***
• The cybersecurity strategy is compatible with the port's vision and mission		***N***
Average Score	***05/20***	
STRUCTURE		
• Clear integration and coordination mechanisms	***Y***	
• Job allocation and authority to do the cybersecurity related jobs	***Y***	
• Simple organization structure of the port	***Y***	
• Decentralized decision making process		***N***
Average Score	***15/20***	
SYSTEM		
• Availability of measurement and control mechanisms for cybersecurity strategy implementation		***N***

• IT and OT systems to assist in cybersecurity strategy implementation	***Y***	
• Monitoring the effectiveness of Cybersecurity strategy implementation		***N***
• An open system: free flow of information between the departments/branches within the port		***N***
Average Score	***05/20***	
STAFF		
• Sufficient number of employees to facilitate the Cybersecurity implementation process		***N***
• Level of education and experience of staff especially in IT/OT/Cybersecurity operation		***N***
• Availability of multi-disciplinary team involved in the Cybersecurity strategy implementation		***N***
• Good working relationship within members of the IT/OT/Cybersecurity team	***Y***	
Average Score	***05/20***	
STYLE		
• Support of key groups and other professionals connected to Cybersecurity		***N***
• Positive attitude of leadership towards the Cybersecurity strategy being implemented	***Y***	
• Sufficient support from Top management in cybersecurity strategy implementation		***N***
• Leadership style allows those involved in Cybersecurity strategy implementation to participate freely		***N***
Average Score	***05/20***	
SKILLS		
• Efficient and sufficient feedback mechanisms	***Y***	

• Availability of relevant IT/OT/Cybersecurity skills and competences within the staff		***N***
• Availability and allocation of financial resources towards cybersecurity strategy implementation		***N***
• Availability of sufficient ways of developing skills in IT/OT/Cybersecurity		***N***
Average Score	***05/20***	
SHARED VALUES		
• Employees' belief in the vision and mission of the organization	***Y***	
• The organization's culture and ability to change	***Y***	
• Employee's awareness of the Cybersecurity strategy being implemented		***N***
• The Cybersecurity strategy is supported by the prevailing local/ national culture		***N***
Average Score	***10/20***	
Overall Score	***50/140***	

The results in Table 5.2 implies that the interviewees concur that simple, clear, and easily understood cybersecurity strategies lead to the success of the process of implementing the strategy, but the rank is quite low in the component of strategy with a 05/20. There is also IT and OT systems to assist in cybersecurity strategy implementation. However, they noted that cybersecurity implementation stages and timeline is ambiguous and complex. There is also a lack of measurement and control mechanisms for cybersecurity strategy implementation. In addition, the respondents indicated that the level of education and experience of staff especially in IT/OT/Cybersecurity operation is still wanting (represented by 05/20 in the staff component) and there is a lack of availability of sufficient ways of developing skills in IT/OT/Cybersecurity.

The findings showed most of the respondents indicated that there was Positive attitude of leadership towards the cybersecurity strategy being implemented but with

insufficient support from top management in cybersecurity strategy implementation (represented by 05/20 in the style component). What is important is that the employees believe in the vision and mission of the organization.

Table 5.3: Kenya/Mombasa Port Analysis using the PESTEL Framework

PESTEL Framework	**Aligned**	
	Yes [05]	***No [0.0]***
POLITICAL FACTORS		
• Government stability/instability	***Y***	
• Corruption in Government	***Y***	
• Favorable Tax policies		***N***
• Government regulation and deregulation	***Y***	
• Appropriate (cyber) defense expenditures		***N***
• Warm bilateral relationships	***Y***	
• Import-export regulation/restrictions		***N***
• Trade control	***Y***	
• Appropriate size of government budgets		***N***
Average Score	***25/45***	
ECONOMIC FACTORS		
• Favorable growth rate	***Y***	
• Federal government budget deficits		***N***
• Low unemployment trend		***N***
• Stock market trends		***N***
• Exchange rate	***Y***	
Average Score	***10/25***	
SOCIAL FACTORS		
• Population size and growth rate		***N***
• Attitudes towards foreign people	***Y***	
• Appropriate Education level	***Y***	
• Attitude towards work	***Y***	

• Wealth distribution		***N***
• Per capita income		***N***
• Average disposable income		***N***
• Attitude towards government		***N***
Average Score	***15/40***	
TECHNOLOGICAL FACTORS		
• Technology incentives		***N***
• Automation		***N***
• R&D activity		***N***
• Technological change		***N***
• Access to new technology		***N***
• Level of innovation		***N***
• Technological awareness	***Y***	
• Internet infrastructure	***Y***	
• Communication infrastructure	***Y***	
• Life cycle of technology		***N***
Average Score	***15/50***	
ENVIRONMENTAL FACTORS		
• Weather	***Y***	
• Climate	***Y***	
• Environmental policies		***N***
• Climate change		***N***
• Pressures from NGO's		***N***
• Natural disasters		***N***
• Air and water pollution	***Y***	
• Recycling standards		***N***
• Attitudes towards green products		***N***
• Support for renewable energy		***N***
Average Score	***15/50***	
LEGAL FACTORS		

• Discrimination laws		***N***
• Antitrust laws		***N***
• Employment laws	***Y***	
• Consumer protection laws		***N***
• Copyright and patent laws	***Y***	
• Health and safety laws		***N***
• Education laws	***Y***	
• Consumer protection laws		***N***
• Data protection laws		***N***
Average Score	***15/45***	
Overall Score	***95/255***	

Kenya as a country is known to be politically stable with favorable Tax policies and growth rate, and warm bilateral relationships (The World Bank, 2021), however there is rampant corruption in Government, high rate of unemployment and low trade control (scoring a 25/45 in the political factors component). The study also noted that the country has got high population size and growth rate with poor wealth distribution. The average disposable income and income per head is also low, scoring a 15/40 in the social factors component. Kenya and Mombasa port in particular fares poorly in the technology factors. Technology incentives, Automation, R&D activity is either nonexistent or very poor, Very low level of innovation and access to new technology. However, the level of technological awareness is fair with fair internet and communication infrastructure (scoring a 15/50 in the technological factors component).

Kenya is also endowed with excellent climate and weather but with poor environmental policies, recycling standards and limited support for renewable energy subsequently scoring 15/50 on the environmental factors component. The country is also known, according to the study for not discrimination, antitrust laws but with limited consumer and data protection laws, scoring 15/45 on the legal factors component.

5.2. Cybersecurity Implementation at Valencia Port

5.2.1. Overview of Valencia Port

The Port Authority of Valencia, popularly known and trading under the name of Valenciaport, is the national body accountable for running and management of three state-owned ports along an 80km stretch of the Mediterranean coast in Eastern Spain: Valencia, Sagunto and Gandía.

The port of Valencia is the first and last port of call for regular shipping lines operating in the Western Mediterranean. As a hub for the entire Western Mediterranean, the port professionally distributes goods over a radius of 2,000km, both in southern EU countries and in North Africa, representative of a huge market of 270 million consumers. The port is highly specialized in the traffic of containerized produce that also attends to other traffics including liquid and solid bulk and ro-ro cargo. The port also manages consistent passenger and merchandise traffic with the Balearic Islands, and receives a large number of cruise ships yearly in its facilities.

Approximately the most significant figures in 2019 for the port of Valencia were around 81 million tonnes of total traffic; 7900 calls vessel; five and a half million of containers (TEU); 1.113.000 passengers and 723.000 vehicles.

With respect to container throughput in 2019 was the fifth port of Europe, the second of the Mediterranean and the first of Spain (Data Ports, 2021). The PAV, as well as other port authorities in Kingdom of Spain, reports to the Ministry of Transportes, Movilidad Agenda town and is ruled by Spanish Legislative Royal Decree 2/2011 of five Gregorian calendar month underneath that the recast text of the Spanish Law on

State-Owned Ports and the Merchant Navy was passed (*Valenciaport.* 2021)

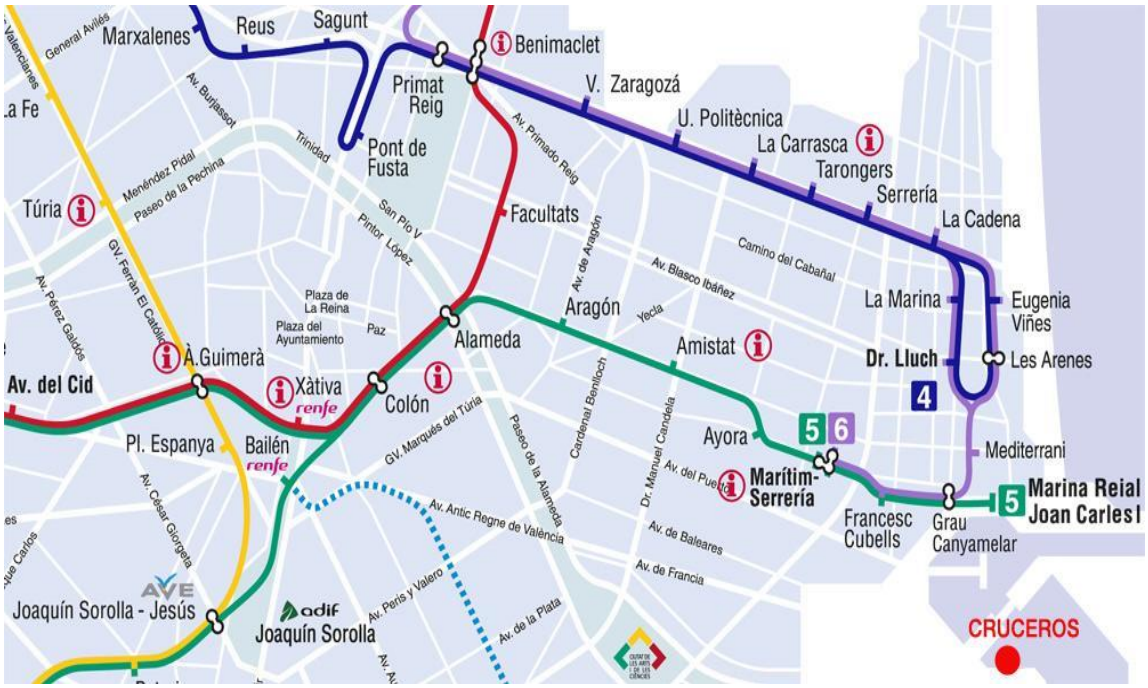

Figure 5.2: Map of Port of Valencia. Maps Valencia. (2021, 08).

5.2.2. Cyber Risk and Threat Management at the Port of Valencia

According to #VAL05, the port addresses 3 key classes of activities:

Maritime shipment connected activities which has general shipment, container, liquid or dry bulk in addition to dedicated infrastructure and services to manage connected operations and welcoming shipment vessels together with unloading and loading, storage, customs scrutiny, and sanitary controls.

Passengers and vehicles transport connected activities laced with dedicated infrastructure and services to welcome vehicles and passengers on ships and manager connected operations like parking, traveler gangways, bars and restaurants, and border management.

Fishing connected activities involving dedicated infrastructure and services to manage and welcome fishing boats and connected operations like fish scrutiny, fish unloading/loading, and fish cold storage.

In an effort to support these varied activities, the Port of Valencia provides main services as portrayed within the Figure 6.: Main services, Activities and Infrastructure at Port of Valencia, (Port du Valencia, 2019). These services and activities area unit assembled into seven classes, and were consequently outline supported through the desktop analysis and knowledge provided by the respondents who contributed to the study.

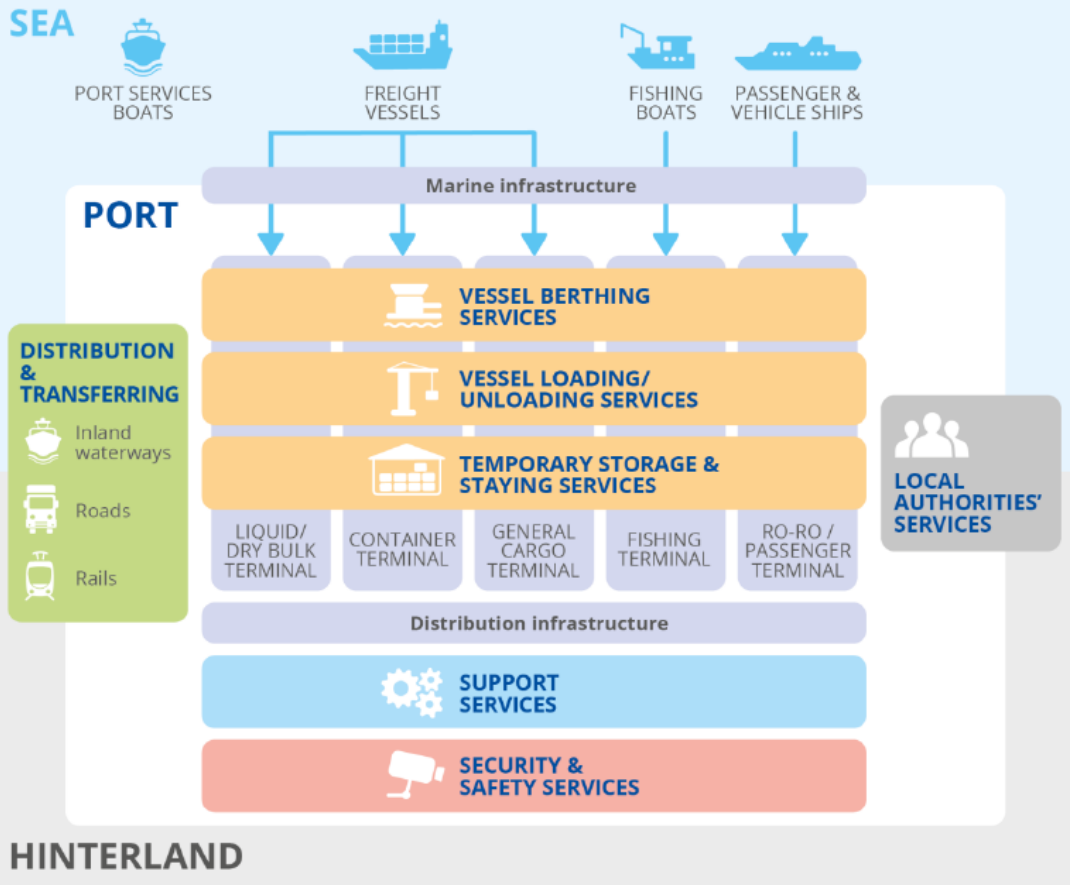

Figure 5.3: Main Services, Activities and Infrastructure at Port of Valencia, (Port du Valencia, 2019)

Some of the cybersecurity risk and threat management approaches at the port of Valencia is detailed below:

Security Operations Management: This is the on-the-ground process by which security incidents at the port are managed, security controls are implemented and maintained, and people with a higher level of access to IT/OT systems and data are subject to oversight. They include: 1) Communication and Reporting; The port's ICT manager

and his team provides management with measurements of success through metrics and key performance indicators (KPIs). Respondent #VAL08 notes that "some of the reports and communication we make to management includes the number of antivirus installations that are complete and up to date and the number of attacks blocked by a firewall in a given period of time". 2) Change Management; The port has got a change management plan in place but in it lacks important components like a change management system and change advisory board (CAB) as advised by international standards like ITIL.

Business Continuity Planning (BCP): On BCP at the port, in order to figure out how IT/OT systems can resume normal operations during a disaster, the business continuity officers are, as reported, works with each business unit at the port as closely as possible. They meet with the people who make the decisions (management), the people who carry out the decisions in IT/OT systems management team, and finally the "worker bees (IT/OT front line staff)" who actually do the work.

Disaster Recovery (DR): On DR, the port works with IT/OT subject matter experts (SMEs), to figure out a way to bypass for example a particular electronic feed or file dependency that may be needed to continue the recovery of a Cybersecurity system. The responsible business continuity or disaster recovery professional works with the IT/OT department and the Cybersecurity unit to achieve one purpose—to operate a fine, productive, and lucrative port. The test involving a Cybersecurity system occurs every 3 months and all the documentation and results from it backed up. Respondent #VAL03 explains:

> We as a port come to know who and what is being recovered by gathering experts together, such as the programmer, business analyst, system architect, or any other SME that is necessary. These experts are invaluable when it comes to creating our DR plan. They are the people who know what it takes to technically run the IT/OT systems in question and they always explain why a certain disaster recovery process will cost a certain amount. This information is important for the CIO/ICT manager of the port, so that she or he can make informed decisions.

Talent and Training: The port employs a reasonable number of talented IS/IT employees with an average of 5-10 years of work experience. However, the IT/OT department at the port is suffering from gaps in critical skills areas such as

cybersecurity, cloud computing and DevOps. IT professionals who have been offered professional development opportunities are struggling to keep up. The blame is always on the rate of technological change which is outpacing training at the port as Respondent #VAL06 noted "We are lacking a culture of continuous learning, team member development, and talent pipeline development in this fast changing lane of technology and financial technology for that matter".

Database Security: The port relies heavily on the information stored in their database systems. From Cybersecurity business transactions to human resources records, and Cybersecurity mission-critical, sensitive data is tracked within these systems. Many of the security-related best practices have been deployed by the port to secure database systems including network-level security, physical security, and using server-related best practices. However, there are additional considerations that should be taken into account when securing databases. They include operating system security, using application security, and database auditing, among others and these are found to be wanting at the port.

Computer Security: The port is using best practices to secure both Windows and Unix systems alike as described by Respondent #VAL04:

> we are doing our best to reduce the attack surfaces, run security software and antiviruses, apply vendor security updates, perform strong authentication, and control administrator privileges. However, out of the box, Windows contains many vulnerabilities that leave it open to attack, but we are trying our best to reduce those vulnerabilities in a number of ways. Whether a server or a workstation, the approach is the same.

What seems to be missing is that the port is failing to separate these systems based on risk which is very important.

5.2.3. SWOT analysis for cybersecurity strategy implementation at Port of Valencia Port

This should be noted that the reasons for this analysis/assessment is to determine the strengths and weaknesses of the Port of Valencia so as to utilize the strengths and reduce the weaknesses. The strengths shall be exploited while the weaknesses are reduced. The factors that are covered by this evaluation are listed in Table 5.4 below:

Table 5.4: SWOT analysis for cybersecurity strategy implementation at Valencia Port

Cybersecurity Strategy Port of Valencia Implementation

INTERNAL FACTORS	
STRENGTHS (+)	**WEAKNESSES (–)**
1. Decarbonization of policy of the port 2. The Open Data Policy of EU Ports 3. Increased state investment in ports 4. Well-developed port community 5. The management of the port has highly qualified staff, trained in the maritime industry. 6. Multipurpose nature of Port of Valencia 7. Advanced logistics practices and high solution capacity 8. Reduced cost of operation and maintenance 9. Increased safety of the port compared to other EU ports 10. Highly developed technological infrastructure that provides favorable conditions for development of the production function in relation cargo handling, production and processing.	1. Vulnerabilities errors such as security and integrity of the port in achieving the Industry 4.0 concept 2. High costs of development and implementation of new technologies 3. Human capital: Manual workers are under the direct influence of process automation inherent to digitalization 4. Lack of strategic planning for cybersecurity 5. Effects of the change in operations. 6. Complications of heterogeneity of applications

		11. Advantageous location in relation to the biggest Spanish economic centers as well as logistics and distribution centers 12. Location of the port in the Pan-European Transport Corridor is advantageous.	
EXTERNAL FACTORS	**OPPORTUNITIES (+)**	**STRENGTHS (+) / OPPORTUNITIES (+) STRATEGY**	**WEAKNESSES (–) / OPPORTUNITIES (+) STRATEGY**
	1. New lines of business in developing markets 2. Technological maturity 3. Synergies port-city 4. Efficient and predictive supply chain 5. Insertion in the global Spanish chain on the 6. Partnership of Spanish ports as connectors of port activity 7. Increase in Spanish foreign trade as a result of the Spanish economic development	Continuous improvement hinged on proven measurement of regular processes, services and products; Consolidating a network of emerging companies and new business lines that develop innovative products for the port sector; Practically apply new innovation strategies; promoting the adaptation and transition from the logistics-port sector to an Industry 4.0 state; Explicit data and information-based approach hinged on sound practices for measurement as a step stone for control port performance. .	Entering innovative national and international ecosystems; Having a corporate start-up incubator for the logistics-port sector; Accessing financing and facilitating the capture of private investment for port innovation; Port personnel must be given the opportunity to act creatively; Need to accommodate both “boat rockers” and “can doers”
	THREATS (–)	**STRENGTHS (+) / THREATS (–) STRATEGY**	**WEAKNESSES (–) / THREATS (–) STRATEGY**

	1. Political and institutional elements 2. Poor integration of other actors in the port sector 3. Changes in legislation, regulations 4. Systems vulnerable to cyber threats 5. Asymmetry with other modes of transport 6. International financial uncertainty	Boost logistical eefficiency in the areas of infrastructure, operations and service provision, improving environmental and energy sustainability, security and protection as well as the digitalization of intelligent processes and platforms	There should be enough time for reflection and introspection; Development of systems including control systems, innovation management information systems, competitor analysis, Appraisal, training and development systems, and recognitions systems.

A SWOT analysis, or, sometimes reversed as TOWS analysis, was performed for the port of Valencia taken together and the result of the analysis is presented in a tabular form (table 5.4) with the following areas covered: infrastructure; transport, shipping, logistics (TSL) market and the administration and management operations sphere. The analyses of the port together with the researcher's experience show that these areas define the competitive position of seaports in Europe. Poor integration of other actors in the port sector is a limitation. The change process towards the new port system and the modification and replacement of facilities has led to an initial sluggishness and ineptitude in port operations.

The IT and OT Systems are vulnerable to cyber threats. From port of Valencia through the internet, the digitalization of the new ecosphere and the growth and development of technologies show that the port is much more vulnerable and subtle to attacks through cyberspace.

The intermodal transport development and inclusion of the port in the network of intermodal terminals in Spain sequentially upsurges her importance in the European and global supply chains. The key constituents which augment the competitive position of the port of Valencia in European market are: suitably designed and executed development strategies, financially sound and connected with the external environment operation and services domains as well as the EU financial resources dedicated to the development of the fully accessible port infrastructure.

5.2.4. GAP Analysis: McKinsey 7-S Framework and PESTEL

This sub-sub-chapter provides the McKinsey 7-S Framework and PESTEL analysis of the port of Valencia in Spain giving the components of the framework and consequently indicating whether the port complies/aligns to or not. Five (points) is given if compliance/alignment is found and zero (0) if there is no compliance/alignment.

Table 5.5: Spanish/Port of Valencia Cybersecurity Strategy Analysis using the McKinsey 7s Framework

McKinsey 7S Framework	**Complies**	
	Yes [05]	***No [0.0]***
STRATEGY		
• Involvement in the cybersecurity strategy formulation	***Y***	
• Simple, clear, and easily understood cybersecurity strategies	***Y***	
• Concise cybersecurity implementation stages and timeline	***Y***	
• The cybersecurity strategy is compatible with the port's vision and mission	***Y***	
Average Score	**20/20**	
STRUCTURE		
• Clear integration and coordination mechanisms		***N***
• Job allocation and authority to do those cybersecurity related jobs	***Y***	
• Simple organization structure of the port	***Y***	
• Decentralized decision making process		***N***
Average Score	***10/20***	
SYSTEM		
• Availability of measurement and control mechanisms for cybersecurity strategy implementation	***Y***	

• IT and OT systems to assist in cybersecurity strategy implementation	***Y***	
• Monitoring the effectiveness of Cybersecurity strategy implementation		***N***
• An open system: free flow of information between the departments/branches within the port	***Y***	
Average Score	***15/20***	
STAFF		
• Sufficient number of employees to facilitate the Cybersecurity implementation process	***Y***	
• Level of education and experience of staff especially in IT and OT operation	***Y***	
• Availability of multi-disciplinary team involved in the Cybersecurity strategy implementation		***N***
• Good working relationship within members of the IT/OT/Cybersecurity team	***Y***	
Average Score	***15/20***	
STYLE		
• Support of key groups and other professionals connected to Cybersecurity	***Y***	
• Positive attitude of leadership towards the Cybersecurity strategy being implemented	***Y***	
• Sufficient support from Top management in cybersecurity strategy implementation	***Y***	
• Leadership style allows those involved in Cybersecurity strategy implementation to participate freely	***Y***	
Average Score	***20/20***	
SKILLS		
• Efficient and sufficient feedback mechanisms	***Y***	

• Availability of relevant IT/OT/Cybersecurity skills and competences within the staff	***Y***	
• Availability and allocation of financial resources towards cybersecurity strategy implementation	***Y***	
• Availability of sufficient ways of developing skills in IT/OT/Cybersecurity	***Y***	
Average Score	***20/20***	
SHARED VALUES		
• Employees' belief in the vision and mission of the organization	***Y***	
• The organization's culture and ability to change	***Y***	
• Employee's awareness of the Cybersecurity strategy being implemented	***Y***	
• The Cybersecurity strategy is supported by the prevailing local/ national culture		***N***
Average Score	***15/20***	
Overall Score	***120/140***	

Strategy adopted by a port is crucial since it determines the changes and methodologies that a port utilizes to attract business, withstand competitive pressure and improve its competitive position. Additionally, the port of Valencia has continuously involved all stakeholders in the cybersecurity strategy formulation, setting in place a simple, clear, and easily understood cybersecurity strategies. The respondents agreed that the port have adopted several strategies to effectively compete and sustain. This component was supported by an average score of 20/20.

The research respondents agreed vastly that good working relationship within members of the IT/OT/Cybersecurity team lead to the success of the process of implementation of cybersecurity strategy, and this is shown by average of 15/20 which suggests there was consistency in the responses of respondents. It was further found that respondents believed to a great extent that there is sufficient number of staff with relevant skills and experience allocated for cybersecurity strategy implementation

process leading to the success of the strategy with a score of 20/20 in the skills component. The respondents also noted that there was availability of relevant skills and competences within the staff that has led to the success of cybersecurity strategy implementation process. This study also tried to find how the organization shared values influenced the success of cybersecurity strategy implementation process. The respondents vastly believed that awareness of the employees of the cybersecurity strategy being implemented has resulted to the success of strategy implementation process with a score of 15/20.

There were efficient and sufficient feedback mechanisms and the staff possess relevant IT/OT/Cybersecurity skills and competences. The respondents also believed in the availability and allocation of financial resources towards cybersecurity strategy implementation and availability of sufficient ways of developing skills in IT/OT/Cybersecurity with an average score of 20/20 in the skills component.

Table 5.6: Port of Valencia Analysis using the PESTEL Framework

PESTEL Framework	**Aligned**	
	Yes	***No***
POLITICAL FACTORS		
• Government stability/instability	***Y***	
• Corruption fight	***Y***	
• Favorable Tax policies	***Y***	
• Government regulation and deregulation	***Y***	
• Appropriate (cyber) defense expenditures	***Y***	
• Warm bilateral relationships	***Y***	
• Import-export regulation/restrictions	***Y***	
• Trade control	***Y***	
• Appropriate size of government budgets	***Y***	
Average Score	***45/45***	
ECONOMIC FACTORS		
• Favorable growth rate	***Y***	
• Federal government budget deficits		***N***

• Low unemployment trend	***Y***	
• Stock market trends	***Y***	
• Exchange rate	***Y***	
Average Score	***20/25***	
SOCIAL FACTORS		
• Population size and growth rate	***Y***	
• Attitudes towards foreign people	***Y***	
• Appropriate Education level	***Y***	
• Attitude towards work	***Y***	
• Wealth distribution	***Y***	
• Per capita income	***Y***	
• Average disposable income	***Y***	
• Attitude towards government		***N***
Average Score	***35/40***	
TECHNOLOGICAL FACTORS		
• Technology incentives	***Y***	
• Automation	***Y***	
• R&D activity	***Y***	
• Technological change	***Y***	
• Access to new technology	***Y***	
• Level of innovation	***Y***	
• Technological awareness	***Y***	
• Internet infrastructure	***Y***	
• Communication infrastructure	***Y***	
• Life cycle of technology	***Y***	
Average Score	***50/50***	
ENVIRONMENTAL FACTORS		
• Weather	***Y***	
• Climate	***Y***	
• Environmental policies	***Y***	

• Climate change	***Y***	
• Pressures from NGO's		***N***
• Natural disasters	***Y***	
• Air and water pollution	***Y***	
• Recycling standards	***Y***	
• Attitudes towards green products	***Y***	
• Support for renewable energy	***Y***	
Average Score	***45/50***	
LEGAL FACTORS		
• Discrimination laws	***Y***	
• Antitrust laws	***Y***	
• Employment laws	***Y***	
• Consumer protection laws	***Y***	
• Copyright and patent laws	***Y***	
• Health and safety laws	***Y***	
• Education laws	***Y***	
• Consumer protection laws	***Y***	
• Data protection laws	***Y***	
Average Score	***45/45***	
Overall Score	***240/255***	

According to the study, Spain is a stable democracy with efficient fight on corruption and favourable tax policies. The country also has got appropriate (cyber) defense expenditures with great bilateral relationships with neighbours, EU and the globe thereby scoring an average of 45/45 on political factors component. This is good for cybersecurity strategy implementation. On the economic factors component, the country is believed to possess favourable growth rate only hindered a little bit by COVID 29 pandemic, but rebounding fast. The country also has got very low unemployment rate with great stock market trends thereby scoring an average of 20/25. The population size and growth rate is favourable and the citizens has got good attitudes towards foreign people, work, but unfavourable attitude towards government

especially with the botched succession plan of Catalonia. The country also has good income per head and disposable income is attractive, scoring 35/40 on the social factors component.

The country of Spain and port of Valencia has got great technology incentives with state of the art automation, high level of innovation and bustling R&D activities. The is excellent response to technological change and access to new technology. The citizens are highly aware of new technological and the internet and communication infrastructure is very good, scoring a whopping 50/50 in the technological factors component. Spain also boasts of good climate and weather, great environmental policies, and attitudes towards green products with an increased support for renewable energy, scoring 45/50 in the environmental factors component. The country has got in place working and efficient Discrimination, Antitrust, Employment, Consumer protection, Copyright and patent, Health and safety, Education, Consumer protection, and Data protection laws - scoring an average of 45/45 in the legal factors component.

5.3. Maritime Cybersecurity Implementation Metrics assessment in developed (Europe) and developing (Africa) Countries

Table 5.7: Cybersecurity threat and risk mitigation measures at the two ports

Control No.	**Control Name**	**Mombasa Port**	**Port of Valencia**
1	Control Policy and Procedures for Access		
2	Management of Accounts		
3	Access Enforcement		
4	Revocation of Access Authorizations		
5	Access enforcement/Controlled release		
6	Information flow enforcement		
7	Information flow enforcement/metadata		
8	Information flow enforcement/Domain Authentication		

9	Information flow enforcement/validation of metadata		
10	Information flow enforcement/physical-logical separation of information flows		
11	Separation of Duties		
12	Least Privilege		
13	Least Privilege/Privileged Access by non-organizational users		
14	Remote Access		
15	Remote Access/Protection of Information		
16	Wireless Access		
17	Access Control for Mobile Devices		
18	Use of External IT and OT		
20	External IT and OT usage/non-organizationally owned systems/components/devices		
21	Sharing of Information		
22	Publicly accessible content		
23	Access control decisions		
24	Policy and procedures covering Security awareness and training		
25	Security training that are Role-based		
26	Physical Security training		
27	Audit and accountability policy and procedures		
28	Audit events		
29	Analysis, Audit review, and reporting		
30	Analysis, Audit review, and reporting/association with information from sources that are non-technical		

31	Non-repudiation		
32	Identity association		
33	Validation of binding of information for producer identity		
34	Non-repudiation connected to chain of custody		
35	Audit generation		
36	Monitoring for information disclosure		
37	Cross-port auditing		
38	Cross-port auditing-that is sharing of audit information		
39	Authorization and Security assessment		
40	Security Assessments		
41	Security Assessments/specialized assessment		
42	External organizations security assessments		
43	Interconnection of systems		
44	System interconnections/Unclassified non-national security system connections		
45	System interconnections/connections to public networks		

The metrics assessment of the two ports under study clearly shows that cybersecurity strategy implementation from a technical/practical point of view targeting cyber threat/risk mitigation is more advanced in Europe - Spain (Port of Valencia) as compared to Africa – Kenya (Port of Mombasa). Both ports demonstrated effective practice on control policy and procedures for access, accounts management, and access enforcement. Other areas where both ports were seen to have acted efficiently in an effort to mitigate cyber threats and risks included: information flow enforcement; domain authentication; separation of duties; least privilege policy; publicly accessible content; remote access; protection of information; wireless access; use of external IT

and OT; access control for mobile devices; non-repudiation connected to chain of custody, and cross-port auditing among others.

However, there are critical areas where port of Valencia beats Mombasa port in compliance, that included; revocation of access authorizations; metadata and validation of metadata information flow enforcement; privileged access by non-organizational users; non-organizationally owned IT/OT systems/components/devices usage; analysis, audit review, and reporting/association with information from sources that are non-technical; identity association; validation of binding of information for producer identity; monitoring for information disclosure; external organizations security assessments; and system interconnections/unclassified non-national security system connections, among others. This puts Port of Valencia in the upper hand compared to Mombasa port in relation to cybersecurity implementation practices.

CHAPTER 6. CONCLUSION AND RECOMENDATION

6.1. Conclusion

With ports globally undergoing rapid digital makeover, cybersecurity has to be observed not simply as a crucial issue to be well thought-out in rapports of custody with the technical developments but on the other hand as a facilitator of additional growths and computerisation.

The previous chapters additionally provide a listing of sensible baseline security measures to strengthen cybersecurity in port operations and systems.

It should be understood that the people responsible for port cybersecurity, that include the CIOs, CISOs, and ICT Managers found in the two Port Authorities.

The models of Cybersecurity measures pursued by European and African ports faces and presents a multitude of challenges and risks including; Infrastructure challenges, talent for Cybersecurity, technology, strategy, governance, product, crime/fraud, reputation, and regulation, among others. However, one outstanding risk is the rapid change in technology and innovation that has greatly affected Cybersecurity strategies in that these strategies become redundant and obsolete before optimal use.

There is need for cybersecurity to be well acknowledged as a significant element of maritime security and should therefore be incorporated into both the European and

African maritime security apparatuses and frameworks. Likewise, as ICTs are being integrated day by day into all facets of human life, significant attention has to be given in detail to the traits of maritime cybersecurity. Cybersecurity in ports in this digital age is becoming more complicated than ever as security technology – including methods to evade it are gaining in sophistication.

European Union and African Union states should at this point work closely with the private sector for efficient and effective sharing of knowledge and understanding with reference to explicit problems faced by the industry. Additionally, the EU and AU should institutionalise the responses of member states in relation to these types of security risks including raising awareness around the vulnerability and cyber threats concerning the maritime sphere.

Kenyan ports have not developed her own comprehensive Cybersecurity reports and are relying on other related reports to monitor some risks that are directly linked to Cybersecurity. They also don't employ a comprehensive approach to Cybersecurity, seldom integrating Cybersecurity strategies in all areas of operations and in the organizational culture. There are also a number of unmet requirements/gaps in the way Cybersecurity systems at the ports are managed.

European and African ports need to prioritize digital risk assessment and reinforce updated Cybersecurity practices to ensure that all data is private, encrypted, and secured appropriately. As government and regulatory bodies are also becoming more aware of the risks and threats to Cybersecurity and other digital operations at ports, regulations and compliance requirements must increase concurrently and ports should be held to a higher standard for maintaining Cybersecurity.

In conclusion therefore, significantly grander energies and consideration should be focused towards making sure Africa and Kenya's cybersecurity is intact. In lieu of that, and given the pervasiveness of non-African indication on maritime cybersecurity incidents, increased Africa-specific knowledge and research is obligatory. This dissertation shall help stakeholders that are active in implementing cybersecurity in ports.

6.2. Summary of Findings

While this study focuses on comparing the cybersecurity implementation practices for ports in developed and developing countries, it also reveals some findings that I hope can contribute to a more sustainable and safer cybersecurity implementation that especially serve low resource countries at scale. I summarize these findings here.

Both ports face a multitude of challenges and risks in cybersecurity implementation that include; talent for cybersecurity, technology, strategy, governance, crime/fraud, reputation, and regulation, among others. The rapid change in technology and innovation has greatly affected cybersecurity implementation strategies in that these strategies become redundant and obsolete before optimal use and the results from this study show very clearly that the port is worried about the potential for technology to do harm by encouraging irresponsible behavior and exploiting lack of IT and OT sophistication.

The study shows that the ports under study are trying to digitize more of its departments, functions, processes and services and to a lesser extent, cybersecurity risk management.

The ports and shipping industry is undergoing rapid technological and digital transformation where such change is improving efficiency and effectiveness.

Mombasa port is not yet dedicating sufficient resources so as to address both the current and future challenges to cybersecurity.

The port of Mombasa lacks specific research and knowledge on maritime cybersecurity even though it is in an advantageous position to learn from developed countries such as Europe-Spain-Valencia port to mitigate future cyber threats and address vulnerabilities.

Mombasa port does not have clearly defined threat/risk management policies and procedures for not only IT/OT/Cybersecurity but also other non-technology risks such

as reputation risk, operational risk and strategic risk that also affects cybersecurity implementation.

The cybersecurity risk management tools being used at Mombasa port are very limited and the port do not have in place an independent review of their cybersecurity implementation functions.

There are no enterprise wide IT/OT/Cybersecurity risk management systems instituted at Mombasa port and in most cases, cybersecurity risks and threats are being managed in silos.

The board at both ports is spending less time on cybersecurity issues and are in most cases not actively engaged and involved in cybersecurity risk policy setting and governance. Cybersecurity risk management is literally not embedded into the "fabric" of both ports.

Mombasa port is, to a larger extent, adding digital technology to older/legacy IT/OT and business processes technology rather than creating separate digital departments or incubator units. This is leading to problems of infrastructure configuration, integration, management and update.

Mombasa port recognizes a lack of resource allocation as the most impeding influence to cybersecurity implementation. They also regret a lack of management awareness and risk aversion to innovation and new technologies.

In conclusion therefore, Cybersecurity threats and risks facing ports in both developing and developed countries are likely to grow and become increasingly complex with ports becoming increasingly reliant on technology to run their operations and services and with the rate of technological change continuing at a very fast pace. Whereas reliance on technology brings obvious benefits, it also evident that ports are increasingly vulnerable to system failures, data losses and cyber-attacks. Trends towards more social networking, the growth of cloud computing, varying and ambiguous (and often lagging) national ICT regulation will only add more salt to injury.

6.3. Recommendation

Ports and ships worldwide are all the time using systems that heavily depend on digitization, automation and integration. Hence, as a consequence, security of data and a number of other sensitive information has come to be a major concern of maritime. Here are some recommendations that will un doubtfully help maintain maritime cyber security in developing countries at the state level and beyond.

a) *Malware Prevention:* Ports and ship owners should implement a fitting policy for anti-malware geared towards in-depth defense in their networks that is both on-board and ashore including filtering out malicious content and unauthorized access.
b) *Management of Incidents:* Is extremely important that a port or ship pin points any source, internal or external that specializes in incident management because evidence and research shows that effective and efficient incident management policies and processes do helps in improving resilience and consequently reducing any impact in relation to maritime cyber security.
c) *Controls directed to removable media:* Policy of removable media is known to; limit the types and also quantity of media that can be used together with the systems, users, and information types that can be moved, control the use of removable media for the import and export of information. So this can be priceless for the ports to implement.
d) *Regime directed to Risk Management:* The are very many benefits associated to embedding an appropriate risk management regime across a port and/or shipping organization. Ports should ensure they clearly communicate their risk management approach through the development policies and practices that are applicable.
e) *Secure configuration:* Another important aspect is that of configuration management which is known to improve the systems security and also eliminate the give and take risk of both them and any information. For that reason, ports should ensure they develop a strategy directed towards removing needless functionality from systems as well as quickly fixing identified vulnerabilities.

f) *Monitoring:* Ports should quickly devise means to detect actual or attempted attacks on systems and services. Monitoring at this juncture allows ports to guarantee that systems are appropriately being used as well as acting in accordance with any regulatory requirement.

g) *Managing user privileges:* At the port, all users need to be provided with a judicious level of privileges and rights to system that are required for each role. It should be understood that the granting privileges of highly raised up system privileges has to be controlled and managed carefully.

h) *Education and awareness of employees:* The port administrators should know that personnel both aboard and ashore do play an important role in relation to cybersecurity therefore it is critical that the technology and rules related to security that are provided should be in position to enable them to do their work. There should be a methodical awareness distribution of programmers and training so as to deliver security expertise and at the same time assist in establishing a culture that is conscious of security.

i) *Remote system access:* Port management should ensure that policies and procedures that are risk based are set up so as to sustain remote access to systems that are also appropriate to service providers. This is critical because remote system access do not only offer countless benefits, but on the other hand it also disclosures new risks. In relation to a number of other digital developments, specialists do recommend collaboration, cooperation and resilience in order to crack through to the right answers when it comes to maritime cyber security

j) The Kenyan government/Mombasa port need to follow best practices by ensuring the cybersecurity of their port infrastructure and also compliance with the International Maritime Organization guidelines for cybersecurity for vessels as is the case with European ports/Port of Valencia.

k) Member states of Africa including Kenya need to ratify and align with the Malabo Convention including increasing efforts to generate the administrative and legal framework it imagines as is the case with European countries/Port of

Valencia and the European Legal Framework. This is because cybersecurity hinge on shared security and capability to deal with risks and threats.

l) Because of the interlocked nature of many regions in areas such as trade and infrastructure, African/Kenyan governments and ports need to become aggressively involved with the regional maritime and cybersecurity institutions. African states need to follow a regional methodology to cyber maritime security as is the case with European ports/Port of Valencia and the European Union.

m) Like how the European Ports and countries conduct maritime cybersecurity related research, African/Kenyan Ports/Mombasa port need to conduct maritime cybersecurity related research so as to address the gap caused by the lack of maritime cybersecurity related research in African states

REFERENCES

Acharjya, D. P., Geetha, M. K., & Sanyal, S. (2017). Internet of things: Novel advances and envisioned applications. https://link.springer.com/book/10.1007%2F978-3-319-53472-5

Agatz, N., Bouman, P., & Schmidt, M. (2018). Optimization approaches for the traveling salesman problem with drone. *Transportation Science, 52*(4), 965-981. https://10.1287/trsc.2017.0791

Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering, 8*(10), 776. https://https://doi.org/10.3390/jmse8100776

Arndt, E. H. (2016). *Fleet support center ist riesenschritt.* https://www.thb.info/rubriken/detail/news/fleet-support-center-ist-riesenschritt.html

Azadeh, K., De Koster, R., & Roy, D. (2019). Robotized and automated warehouse systems: Review and recent developments. *Transportation Science, 53*(4), 917-945. https://10.1287/trsc.2018.0873

Balduzzi, M. (2014). AIS exposed understanding vulnerabilities & attacks 2.0. *Blackhat Asia*, Port of Valencia Map. https://www.Valencia-tourist-guide.com/en/transport/cruise-port/map-of-Valencia-port.html

Baltic and International Maritime Council. (2020). The guidelines on cyber security onboard security ships. https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/guidelines-on-cyber-security-onboard-ships-v4.ashx

Bendel, O. (2015). Die industrie 4.0 aus ethischer sicht. *HMD Praxis Der Wirtschaftsinformatik, 52*(5), 739-748. https://https://doi.org/10.1365/s40702-015-0163-z

Berg, D., & Hauer, M. (2015). *Digitalisation in shipping and logistics.* https://www.munichre.com/topics-online/en/mobility-and-transport/transportation-of-cargo/digitalisation-shipping-logistics.html

BIMCO. (2016). *The guidelines on cyber security onboard ships.* https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

BMBF. (2018). Industry 4.0. https://www.bmbf.de/bmbf/de/forschung/digitale-wirtschaft-und-gesellschaft/industrie-4-0/industrie-4-0

Broy, M. (2010). Cyber-physical systems—wissenschaftliche herausforderungen bei der entwicklung. *Cyber-physical systems* (pp. 17-31). Springer. https://https://doi.org/10.1007/978-3-642-14901-6_2

Burt, T. (2020). Microsoft report shows increasing sophistication of cyber threats. URL https://blogs. microsoft. com/on-theissues/2020/09/29/microsoft-digital-defensereport-cyber-threats.

Cheung, K., & Bell, M. G. H. (2021). Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study. *European Journal of Operational Research, 291*(2), 471-481. https://10.1016/j.ejor.2019.10.019

Container x-change. (2020,). Sustainable ports: Supporting environomy. https://container-xchange.com/blog/sustainable-ports-environomy/

Culot, G., Nassimbeni, G., Orzes, G., & Sartor, M. (2020). Behind the definition of industry 4.0: Analysis and open questions. *International Journal of Production Economics, 226*, 107617. https://10.1016/j.ijpe.2020.107617

Data Ports. (2021). Port of valencia. https://dataports-project.eu/port-of-valencia/

Department of Transport. (2011). Guidance to UK flagged shipping on measures to counter piracy, armed robbery and other acts of violence against merchant shipping. http://www.fortunes-de-mer.com/mer/images/documents%20pdf/legislation/Internationale/Piraterie/measures-to-counter-piracy.pdf

Dyryavyy, Y. (2015). Preparing for cyber battleships - electronic chart display and information system security. https://www.nccgroup.trust/uk/our-research/preparing-for-cyber-battleships-electronic-chart-display-and-information-system-security/

ECDIS: Navigation in 2018. (2018). https://www.porttechnology.org/technical-papers/ecdis_navigation_in_2018/

Eriksson, P., & Kovalainen, A. (2015). *Qualitative methods in business research: A practical guide to social research*. Sage.

Directive 2005/65/EC of the european parliament and of the council of 26 october 2005 on enhancing port security (text with EEA relevance), (2005). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005L0065

Directive 2010/65/EU of the european parliament and of the council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the member states and repealing directive 2002/6/EC text with EEA relevance, (2010). http://data.europa.eu/eli/dir/2010/65/oj/eng

European Union Agency for Cybersecurity, (ENISA). (2020). Cybersecurity in the maritime sector: ENISA releases new guidelines for navigating cyber risk. https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-maritime-sector-enisa-releases-new-guidelines-for-navigating-cyber-risk

Fraunhofer. (2021). *Digitisation and port technology - port of the future - CML*. https://www.cml.fraunhofer.de/en/fields-of-activity/Ports-and-Transport-Markets/digitisation-and-port-technology---port-of-the-future.html

Frøystad, C., Bernsmed, K., & Meland, P. H. Protecting future maritime communication. Paper presented at the *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 1-10. https://https://doi.org/10.1145/3098954.3103169

Gallagher, J. (2017). Maritime cyber policy in spotlight after maersk attack. https://fairplay.ihs.com/safety-regulation/article/4288491/maritime-cyber-policy-inspotlight-after-maersk-attack.

Global Institute of Logistics. (2017). Port benchmarking group, available at www.globeinst.org/chainport/ (accessed 4 june 2019)., 1. www.globeinst.org/chainport/ (accessed 4 June 2019).

Greer, C., Burns, M., Wollman, D., & Griffor, E. (2019). Cyber-physical systems and internet of things. national institute of standards and technology, US department of commerce. . https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf [accessed 08 June 2021].

Gürel, E. (2017). Swot analysis: A theoretical review. *Journal of International Social Research, 10*, 994-1006. https://10.17719/jisr.2017.1832

Hellenic Shipping News. (2020). Maritime cyber attacks increase by 900% in three years. https://www.hellenicshippingnews.com/maritime-cyber-attacks-increase-by-900-in-three-years/#:~:text=Cyber%2Dattacks%20on%20the%20maritime,record%20volumes%20by%20year%20end.

Hopcraft, R., & Martin, K. M. (2018). Effective maritime cybersecurity regulation – the case for a cyber code. *Journal of the Indian Ocean Region, 14*(3), 354-366. https://10.1080/19480881.2018.1519056

Infomaritime. (2021). Visualization for world merchant fleet data (2016 -2021). http://infomaritime.eu/index.php/2021/08/22/top-15-shipowning-countries/

International Maritime Organisation. (2011). Piracy and armed robbery against ships in waters off the coast of somalia. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC.1-Circ.1339.pdf

International Maritime Organisation. (2017). *Guidelines on maritime cyber risk management*. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

Jahn, C., Bosse, C., & Schwientek, A. (2011). Relevance of information and communication solutions. maritime shipping 2020 - current trends and developments, fraunhofer-center für maritime logistik und dienstleistungen CML, stuttgart: Fraunhofer. http://www2.ciando.com/img/books/extract/3839612063_lp.pdf

Keller, M., Pütz, S., & Siml, J. (2012). Internet der dinge . *(A. Mehler-Bicher & L. Steiger, Hrsg.), Trends in Der IT, Fachhochschule Mainz.*, (pp. 118–122). https://trends-in-der-it.de/downloads/Buch%20trends%20in%20der%20IT%20Final.pdf#page=118

Kianieff, M., Taylor, & Francis. (2019). Blockchain technology and the law: Opportunities and risks. . https://books.google.se/books?hl=sv&lr=&id=DPaODwAAQBAJ&oi=fnd&pg=PT7&dq=Kianieff,+M.+(2019).+Blockchain+Technology+and+the+Law:+Opportunities+and+Risks.+Taylor+%26+Francis.&ots=jMNi3MYfxj&sig=B6ZEV6LGtjhdS28WsXAM2cJG9qk&redir_esc=y#v=onepage&q=Kianieff%2C%20M.%20(2019).%20Blockchain%20Technology%20and%20the%20Law%3A%20Opportunities%20and%20Risks.%20Taylor%20%26%20Francis.&f=false

Kimberly, T., Jones, K., & Papadaki, M. (2016). Threats and impacts in maritime cyber security ., 1-3. http://hdl.handle.net/10026.1/4387

Lag, S., Andersen, P., Vartdal, B., & Knutsen, K. E. (2015). Ship connectivity. *DNV GL Strategic Research & Innovation Position Paper, 4*, 1-48. https://www.researchgate.net/publication/280830264_Ship_Connectivity

Lehto, M. (2020). Cyber security in aviation, maritime and automotive. *Computation and Big Data for Transport,* 19-32. doi:10.1007/978-3-030-37752-6_2

Lennane, A. (2020). Toll group resists ransom demands from hackers after cyber attack. https://theloadstar.com/toll-group-resists-ransom-demands-from-hackers-after-cyber-attack/

Li, S., Li, D. X., & Zhao, S. (2015). The internet of things: A survey., Information Systems Frontiers 17.2 (2015): 243-259. https://https://doi.org/10.1007/s10796-014-9492-7

Li, & Zhou, H. (2020). A survey of blockchain with applications in maritime and shipping industry.https://https://doi.org/10.1007/s10257-020-00480-6

Lloyd's Register. (2017). *HHI announces revolutionary development of ISSS for shipping - lr.org.* https://www.lr.org/en/latest-news/hyundai-heav-industries-announces-integrated-smart-ship-solution/

MARSH. (2014). Research & briefings. https://www.marsh.com/uk/insights/research/the-risk-of-cyber-attack-to-the-maritime-sector.html

Marshall, C., & Rossman, G. B. (2014). *Designing qualitative research*. Sage publications.

Mindtools. (2020). *The McKinsey 7-S framework: - Making every part of your organization work in harmony.* http://www.mindtools.com/pages/article/newSTR_91.htm

Morrow, R., Rodriguez, A., & King, N. (2015). Colaizzi's descriptive phenomenological method. the psychologist., 28(8), 643-644. http://eprints.hud.ac.uk/id/eprint/26984/1/Morrow_et_al.pdf

NIST. (2018). NIST cybersecurity framework compliance with alien vault USM anywhere. https://www.nist.gov/cyberframework

Port of Rotterdam. (2018). "Just-in-time" sailing saves hundreds of thousands of tonnes of CO2 [carbon dioxide], . https://www.portofrotterdam.com/en/news-and-press-releases/just-time-sailing-saves-hundreds-thousands-tonnes-co2

Reva, D. (2020). *Maritime cyber security: Getting Africa ready.* https://issafrica.org/research/africa-report/maritime-cyber-security-getting-africa-ready

Ringsberg, A. H., & Cole, S. (2020). Maritime security guidelines: A study of Swedish ports' perceived barriers to compliance. *Maritime Policy & Management, 47,* 388-401. https://www.tandfonline.com/doi/full/10.1080/03088839.2020.1711977

Robert Lemos. (2019). *Coast guard warns shipping firms of maritime cyberattacks.* https://www.darkreading.com/vulnerabilities-threats/coast-guard-warns-shipping-firms-of-maritime-cyberattacks

Rose, A., DiRenzo III, J., Drumhiller, N. K., & Roberts, F. S. (2017). Economic consequence analysis of maritime cyber threats. *Issues in Maritime Cyber Security*, 321-356. https://westphaliapress.org/2017/06/26/issues-in-maritime-cyber-security/

Salem, A. (2018). Pestle analysis introduction. https://www.researchgate.net/publication/327871826_pestle_analysis_introduction

Eschewer, D., & Sahl, J. (2016). The network needs trust and security. in F. abolhassan (ed.), what is driving digitization? why there is no getting around the cloud. *Wiesbaden: Springer*, 42–44. https://link.springer.com/chapter/10.1007/978-3-658-10640-9_3

Sheffield Hallam University. (2019,). Professional services capability framework: Seeing the bigger picture. https://blogs.shu.ac.uk/shupdreviewtoolkit/files/2019/02/Seeing-the-bigger-picture-single-capability-example1.pdf

Tam, K., & Jones, K. D. (2018). Maritime cybersecurity policy: The scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, *3*(2), 147-164. https://10.1080/23738871.2018.1513053

Tanya, S., & David, G. (2015). SWOT analysis. *Wiley encyclopedia of management* (pp. 1-8). American Cancer Society. https://https://doi.org/10.1002/9781118785317.weom120103

Teegavarapu, S., Summers, J. D., & Mocko, G. M. Case study method for design research: A justification. case study method for design research: A justification. proceedings of the ASME 2008 international design engineering technical conferences and computers and information in engineering conference. Paper presented at the 495-503. https://10.1115/DETC2008-49980 https://asmedigitalcollection.asme.org/IDETC-CIE/proceedings/IDETC-CIE2008/43284/495/329310

The Computer Society. (2020,). 5 cybersecurity threats to be aware of in 2020. https://www.computer.org/publications/tech-news/trends/5-cybersecurity-threats-to-be-aware-of-in-2020/

The Maritime Executive. (2020). *Report: Maritime cyberattacks up by 400 percent.* https://www.maritime-executive.com/article/report-maritime-cyberattacks-up-by-400-percent

The Swedish Club. (2021). *Cyber security and unseaworthiness: What it will mean for owners in 2021*. https://www.swedishclub.com/loss-prevention/cyber-security

The World Bank. (2021). *Overview of the world bank in Kenya.* https://www.worldbank.org/en/country/kenya/overview

Toll, J. (2020). *Blockchain and the future of the maritime industry*. https://www.nasdaq.com/articles/blockchain-and-the-future-of-the-maritime-industry-2020-10-14

Trevor, J. (2021,). Mombasa. https://africaports.co.za/mombasa/

UNCTAD. (2019). Digitalization in maritime transport: Ensuring opportunities for development. *Unctad*, https://unctad.org/webflyer/digitalization-maritime-transport-ensuring-opportunities-development

Valenciaport. (2021). https://www.valenciaport.com/en/port-authority-valencia/about-valencia-port/about-us/

Viano, E. C. (2017). Cybercrime, organized crime, and societal responses. *International Approaches, Basel,* 3-22. https://link.springer.com/book/10.1007%2F978-3-319-44501-4

Vom, B., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., & Cleven, A. Reconstructing the giant: On the importance of rigour in documenting the literature search process. Paper presented at the *17th European Conference on Information Systems (ECIS),*

World Economic Forum. (2020). The global risks report 2020. https://www.weforum.org/reports/the-global-risks-report-2020

Ying Tan, Steve M Goddard, & Lance C Pérez. (2008).. A prototype architecture for cyber-physical systems. ACM signed review 5 (1), 1–2., 1-2. https://doi.org/10.1145/1366283.1366309